СПЕЦИАЛЬНЫЙ ВЫПУСК!

www.upweek.ru



#44 (496)
8 ноября 2010

еженедельный журнал о компьютерах и компьютерных технологиях

ВСЕ, ЧТО ВЫ ХОТЕЛИ ЗНАТЬ О СЕТЯХ, НО БОЯЛИСЬ СПРОСИТЬ

НАСТРОЙКА СЕТИ В ОС LINUX

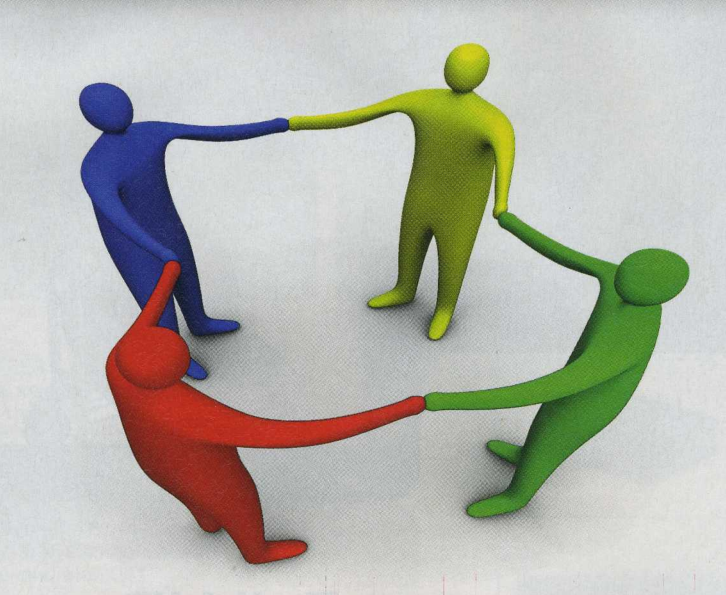
ЭТО НЕ ТАК СЛОЖНО, КАК МОЖЕТ ПОКАЗАТЬСЯ НА ПЕРВЫЙ ВЗГЛЯД

САМ СЕБЕ АДМИН

ПРИНЦИПЫ ОРГАНИЗАЦИИ РАЗНОТИПНЫХ СЕТЕЙ ОТ А ДО Я

БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ

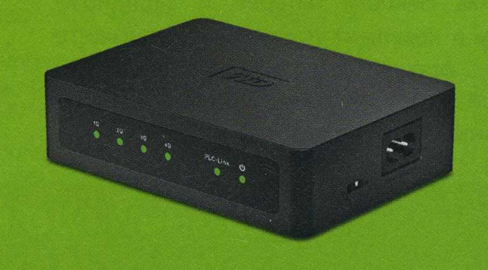
КАК ЗАЩИТИТЬ СВОЙ КОМПЬЮТЕР ОТ ПРОБЛЕМ



СОЗДАЕМ ДОМАШНЮЮ СЕТЬ



СЕТЕВОЙ ТВ-АДАПТЕР AIR 7120: HDTV НА ТВ БЕЗ ИСПОЛЬЗОВАНИЯ ПК



КОМПЛЕКТ СЕТЕВЫХ АДАПТЕРОВ WD LIVEWIRE: ИНТЕРНЕТ ПО ЭЛЕКТРОСЕТИ





#44 (496), 2010
Издается с 1 января 2000 года
Выходит один раз в неделю
по понедельникам

Адрес редакции
129090, г. Москва, ул. Гиляровского, д. 10, стр. 1,
тел. (495) 681-1684,
факс (495) 681-1684
upgrade@upweek.ru
www.upweek.ru

Редакционная политика
Перепечатка материалов или их фрагментов допускается только по согласованию с редакцией в письменном виде. Редакция не несет ответственности за содержание рекламы. Мнение редакции не обязательно совпадает с мнением авторов и художников. Редакция вступает в переписку с читателями, но не гарантирует моментального ответа. Мы будем рады вашим пресс-релизам, присланным на e-mail upgrade@upweek.ru.

Журнал зарегистрирован в Федеральной службе по надзору за соблюдением законодательства в сфере массовых коммуникаций и охране культурного наследия. Регистрационное свидетельство ПИ № ФС77-26571 от 7 декабря 2006 г.

Подписка на журнал UPgrade по каталогу агентства «**Роспечать**» (подписной индекс – **79722**), по каталогу «**Почта России**» (подписной индекс – **99034**).

Старые номера журналов можно приобрести по адресу: м. «Савеловская» Выставочный компьютерный центр (ВКЦ) «Савеловский», киоск у главного входа. Часы работы киоска: ежедневно, с 10:00 до 20:00.

Уважаемые победители конкурсов и авторы писем, опубликованных в рубрике «Почтовый ящик»! Для получения призов вы должны связаться с редакцией в течение одного месяца с момента выхода журнала, из которого вы узнали о своем выигрыше.

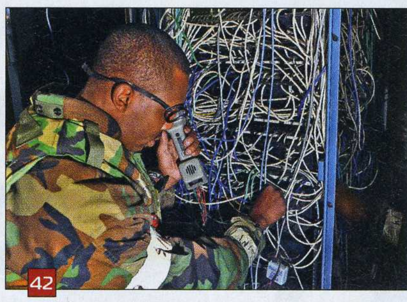
Издание отпечатано
ЗАО «Алмаз-Пресс»
Москва, Столярный пер., д. 3,
тел. (495) 781-1990, 781-1999

Тираж: 92 000 экз.


14



24


42



напиток
коктейль «Молодильное яблоко»

книжка
Эверетт Тру – «Nirvana. Правдивая история»

песня
John Cale – Hallelujah

ссылка
bestphotographer.ru

блог
community.livejournal.com/ru_oldgames

Сеть как она есть

Компьютерные сети – тема всеобъемлющая, и прежде всего надо выбрать, с чего начать рассказ о них. Пожалуй, с определения. Сеть – это структура, позволяющая вычислительным машинам взаимодействовать между собой, отправлять и принимать данные и команды.



DjFedos
hard@upweek.ru
Mood: кочевое
Music: «Цыгане Ивановичи»



Сети в обязательном порядке включают в себя сами компьютеры, носитель (среду передачи) информации и, чаще всего, дополнительное сетевое оборудование. Классифицируются сети в первую очередь по размеру: они делятся на локальные (LAN, Local Area Network) и глобальные (WAN, Wide Area Network). И в этом материале речь пойдет в основном о локальных сетях, поскольку они ближе к пользователю и с их настройкой и применением связано больше всего вопросов. Об устройстве глобальных будет рассказано по мере надобности, тоже по большей части с прикладной точки зрения.

Модель для сетки

Для того чтобы компьютеры и сетевое оборудование могли понимать друг друга, были придуманы протоколы компьютерных сетей. А для того, чтобы разобраться с ними, надо для начала ознакомиться с моделью сети. Модель сети – это абстракция, в виде которой можно представить сеть. Международная организация по стандартизации (International Organization for Standardization, ISO) приняла в качестве эталонной сетевой модели OSI (Open Systems Interconnection Basic Reference Model). Модель OSI устроена сложно – она состоит из семи уровней и грешит оторванностью от реального устройства современных сетей, что неудивительно, так как она была разработана давно. Она достаточно подробно описана в «Википедии», к которой и отсылаю наиболее любопытных читателей. Более близкая к делу модель DOD (Department of Defence, то есть Министерства обороны) была разработана соответствующим ведомством США. Согласно ей устроен стек протоколов TCP/IP, на котором основывается интернет. Именно ее, в применении к TCP/IP, и рассмотрим подробно.

Только для начала определимся с тем, что такое протокол. Протокол сети – это набор правил, по которым происходит обмен данными между компьютерами. Это похоже на использование языка: например, следуя правилам орфографии, люди пишут слова без ошибок, и другой человек может их прочитать. Так же и компьютеры, когда держат связь по набору (стеку) протоколов TCP/IP, без проблем понимают друг друга.

Макет, который оказался сильней

Сетевая модель состоит из уровней, упорядоченных по вертикали. Чем выше уровень, тем он ближе к пользователю. Каждый протокол действует на определенном уровне сетевой модели, хотя из-за того, что сетевая модель абстрактна, некоторые протоколы не удается четко приписать к одному уровню – тогда их приписывают к двум соседним одновременно.

Протоколы более низкого уровня вкладывают в себя высокоуровневые протоколы по принципу матрешек. Такая вложенность называется латинским словом «инкапсуляция», что переводится как «вкладывание», «упаковка». Модель DOD имеет четыре уровня, протоколы первого инкапсулируют протоколы второго и т. д. Это можно сравнить с работой почты. Письмо – пакет информации самого высокого уровня, ближе всего к адресату и отправителю, вкладывается, то есть инкапсулируется, в конверт. Конверт с адресом и индексом – более низкий уровень, дальше от пользователей почты. Он упаковывается в контейнер, вместе с другими конвертами, которые уйдут в том же направлении. Затем контейнер помещается в почтовый вагон поезда. Поезд доставляет контейнер в нужный город, там его разгружают, вынимают из него конверт и доставляют по нужному адресу. А получатель может вынуть из конверта само письмо и прочесть. Примерно так же происходит с пакетами информации.

Самый нижний уровень модели DOD называется уровнем сетевого доступа (Network Access). Он соответствует двум уровням модели OSI: физическому и канальному. Уровень сетевого доступа от-

RSS

ЛВС – локальная вычислительная сеть, или локалка, то же самое, что по-английски называется LAN. Эта аббревиатура будет встречаться вам и в тексте статьи, и в жизни. А глобальную сеть обычно называют просто интернетом. Или WAN.

Про этот номер

В современном мире компьютер без доступа в сеть – вещь довольно-таки инвалидная. Поэтому мы решили свести воедино в одном номере всякие полезности относительно сетей в целом. Это тот самый второй тематический номер, который мы вам обещали. Мы целиком посвятили его сетям и всем вопросам, которые возникают в процессе прокладки, настройки и всей остальной деятельности, направленной на то, чтобы компьютеры видели друг друга, а также были в интернете. Надеемся, что он будет для вас полезен и поможет сохранить время и нервы, которые (мы это знаем по собственному опыту) расходуются со скоростью километр в минуту, когда все должно работать, но на самом деле не работает.

Хорошего вам пинга!

вечает за доставку данных к физическим сетевым устройствам, таким как сетевые адаптеры, в виде кадров (фреймов, от англ. frame). На нем работают такие протоколы, как Ethernet, IEEE 802.11 (известный как Wi-Fi) и 802.16 (WiMAX), а также некоторые другие, не столь привычные для большинства юзеров. Они служат для того же, для чего обыкновенной почте нужны поезда, самолеты и курьеры, – то есть выступают в качестве транспорта. На следующем, втором уровне модели DOD происходит передача сообщений между сетями, в том числе разнородными по устройству. Этот уровень носит гордое название Internet (межсетевой) и сопоставляется сетевому уровню модели OSI. Именно на нем вольготно расположился протокол IP, отвечающий за доставку пакетов информации в современных компьютерных сетях, в том числе в глобальной сети интернет. Он будет достаточно подробно описан ниже, потому что важность IP для компьютерных сетей сложно переоценить.

Прежде всего следует иметь в виду, что протокол IP не гарантирует доставку всех пакетов данных в той последовательности, в какой они были отправлены. Пакет может потеряться по дороге, или, наоборот, продублироваться, или прийти не в свою очередь – протокол IP не имеет контроля за такими ошибками. Поэтому выше располагаются протоколы транспортного уровня (Transport) модели DOD, который соответствует одноименному уровню OSI. Два самых известных протокола транспортного уровня – TCP и UDP. Об их особенностях будет рассказано в материале «Построение сетей от 0 до 1».

Верхний, четвертый уровень DOD охватывает целых три уровня модели OSI (сеансовый, уровень представления и прикладной). Это прикладной уровень, именно на нем расположены протоколы доставки веб-контента (HTTP, HTTPS), файлов (FTP, BitTorrent), электронной почты (POP3, IMAP), а также удаленного администрирования (SSH, Telnet). Все эти, а также многие другие протоколы инкапсулируются в TCP и UDP. Вам интересно, каким образом определяется, по какому протоколу прикладного уровня передается конкретно вот этот сегмент данных TCP или UDP? Тогда читайте дальше.

Порт приписки

Дело в том, что каждому протоколу верхнего уровня приписан определенный порт TCP и / или UDP, реже несколько. Про такое понятие, как порт, слышали многие пользователи компьютерных сетей, но что это такое, не всем известно. Так вот: порт – это номер, который по возможности однозначно (во избежание путаницы) сопоставляется с протоколом верхнего уровня. Сопоставлением портов TCP и UDP с определенными протоколами прикладного уровня занимается IANA (Internet Assigned Numbers Authority, Администрация адресного пространства

интернет). Эта организация еще будет упомянута в связи с управлением IP-адресацией.

Каждый сегмент данных TCP или UDP надписывается номером порта получателя и порта отправителя – «обратным адресом», на который приходят ответные пакеты. Например, отправляя пакеты данных по HTTP, программы надписывают их номером порта получателя 80. Номер порта отправителя не стандартизирован – он генерируется автоматически каждый раз при новом соединении и затем используется.

Итак, с тем, как разобраться с протоколами прикладного уровня, «седлающими» TCP и UDP, все более или менее ясно. А вот как отличить пакеты TCP и UDP, упакованные в пакеты IP? Оказывается, у TCP, UDP и других менее известных и популярных протоколов транспортного уровня есть номера-идентификаторы – по смыслу типа портов. Они прописываются в IP-пакет, чтобы было ясно, что в него инкапсулировано.

Несколько забегая вперед, добавлю, что к открытию или закрытию тех или иных портов TCP и UDP сводится, по большей части, деятельность файрволлов (брандмауэров). Эти программы, как на компьютерах сети, так и на роутерах и межсетевых шлюзах, служат для защиты от хакерских атак. При этом на шлюзе можно блокировать порты как со стороны интернета, чтобы не допустить прохождения ненужных данных в ЛВС, так и со стороны локалки, если есть необходимость. Можно закрывать и открывать порты для определенных IP-адресов своей сети или их диапазонов. Подробнее об IP-адресах и интернет-шлюзах написано далее, а их практическое применение разобрано в «Практикуме» по сетям.

Мой адрес – не дом и не улица

Как компьютер определяет, по каким протоколам извлекать из IP-пакета сегмент транспортного уровня и согласно какому протоколу прикладного уровня обрабатывать его дальше, мы уже знаем. А вот как пакет информации попадает на нужный компьютер, точнее нужный сетевой интерфейс?

Именно для пересылки данных на нужный сетевой интерфейс и служит протокол IP (Internet Protocol). Это протокол сетевого уровня модели OSI и межсетевого – модели DOD. На данный момент больше всего распространена его четвертая версия, однако мир медленно, но верно готовится переходить на более продвинутую шестую. Итак, каким же образом пакет, отправленный с одного сетевого интерфейса, попадает на другой?

В привычной нам четвертой версии протокола адрес сетевого интерфейса имеет вид наподобие 213.180.204.11 – четыре числа от 0 до 255, разделенных точками. На самом деле каждое число от 0 до 255 – это 8 бит, то есть IP-адрес состоит из четырех фрагментов по 8 бит (октетов), а всего из 32 бит. Соответственно, пакет IP содержит IP-адреса получателя и отправителя. В пределах сети каждый сетевой интерфейс снабжается уникальным IP-адресом. То есть в интернете не может быть двух компьютеров с одинаковыми айпишниками, так же, как их не может быть в отдельно взятой локальной сети. При этом в разных локалках могут встречаться сетевые карты с одинаковыми IP-адресами. В интернете они напрямую не видны. Для передачи пакетов IP между разными сетями, например между локалкой и интернетом, используются маршрутизаторы (они же роутеры). О том, как они в общих чертах работают, будет написано ниже.

В интернете одновременно не может быть двух компьютеров или других устройств с одинаковыми IP-адресами, так же, как их не может быть в отдельно взятой локальной сети.

Для использования в локалках выделено три специальных IP-диапазона: 192.168.0.0-192.168.255.255, 172.16.0.0-172.31.255.255, 10.0.0.0-10.255.255.255. Адреса из этих множеств отличаются тем, что в адресном пространстве глобальной сети интернет они отсутствуют. Это было сделано для того, чтобы при подключении нескольких машин одной локальной сети через общий шлюз (см. его определение ниже) не выделять интернет-адрес на каждую. Благодаря этому адресов IPv4 хватало на всех до самого недавнего времени. Таким образом, при построении локальной сети адреса ее устройствам назначаются из одного из этих множеств, в зависимости от размера ЛВС. В малых офисных и домашних сетях используется диапазон 192.168.0.0-192.168.255.255. В районных часто выдают IP-адреса от 172.16.0.0 и до 172.31.255.255.

IP – маршрутизируемый протокол. Это значит, что IP-пакеты могут переходить из одной сети в другую, например из локальной в глобальную и наоборот. Для этого применяются специальные аппаратные и программные средства – маршрутизаторы и межсетевые шлюзы. По идее, это разные вещи, однако на данный момент в малых сетях шлюзами между ЛВС и интернетом служат чаще всего маршрутизаторы, поэтому подробнее остановимся именно на них. Все они умеют направлять входящие пакеты из интернета на нужную машину в локальной сети и, наоборот, адресовать пакеты изнутри ЛВС на нужный сетевой интерфейс в интернете. За этот процесс отвечает механизм трансляции (перевода) сетевых адресов Network Address Transfer (NAT).

При соединении нескольких компьютеров малой офисной или домашней сети с интернетом через маршрутизатор или другой шлюз (см. RSS) машинам и другим устройствам сети выдаются IP-адреса из зарезервированных под эти цели диапазонов (они приведены выше). Их можно либо вручную прописать на каждой машине, либо раздать автоматически. Для раздачи адресов без «рукоприкладства» существует протокол DHCP (Dynamic Host Configuration Protocol, протокол динамической конфигурации узла). Он поддерживается всеми современными ОС (как Windows, так и GNU / Linux, и Mac OS). Во многие, если не во все имеющиеся в продаже, роутеры встраивают DHCP-сервер, автоматически раздающий IP-адреса и другие необходимые настройки сети всем подключающимся к

Примеры портов для протоколов **прикладного** уровня

HTTP	80, 8080 TCP
HTTPS	443 TCP
FTP	20 (данные), 21 (команды) TCP
SSH, SFTP	22 TCP, UDP
DNS	53 TCP, UDP
POP3	110 TCP
ICQ	5190 TCP

RSS

Межсетевым шлюзом может быть не только аппаратный роутер. Те же функции может выполнять, например, компьютер, для чего необходимо установить подходящий софт и настроить его. Интернет-шлюзы на GNU / Linux порой используются в офисных ЛВС.

ней компьютерам и другим девайсам (если они сами по себе поддерживают DHCP). При этом админ может без проблем настроить сервер дополнительно, задав диапазон, из которого будут выдаваться адреса.

А если все же выдавать IP-адреса (из тех же диапазонов, кстати) вручную, то делать это нужно с умом. И об этом тоже будет рассказано в статье Конструктора.

Имена и номера

Рассмотрев более прицельно настройку локальной сети, а именно выдачу ее устройствам (не только компьютерам, см. RSS) адресов в совокупности с масками подсети, мы отвлеклись от темы глобальных вычислительных сетей. Самое время вернуться к ним, точнее к ней – к сети интернет.

Мы узнали, что в локальных сетях используются адреса из специальных множеств, которые не применяются в интернете. А значит, во Всемирной паутине используют другие адреса. Причем делают это не «от балды», а согласно решениям IANA. Эта организация упоминалась выше в связи с припиской портов определенным протоколам прикладного уровня. И она же выдает айпишники крупным региональным регистраторам, которые раздают их более мелким компаниям, а они уже приписывают IP-адреса «большого интернета» конкретным ресурсам. Между прочим, запас свободных IPv4-адресов подошел к концу, и именно из-за этого постепенно внедряют IPv6, в котором адреса имеют длину в 128 бит и пишутся обычно восьмью группами по четыре шестнадцатеричных цифры (от 0 до F).

Но вы наверняка замечали, что при работе в сети обращаетесь к ресурсам по буквенным адресам, а не по IP-адресам. И скорее всего, знаете, что существует система, которая переводит близкие людям буквосочетания в понятные машинам цифровые коды, то есть URL (Uniform Resource Locator, неточный, но адекватный перевод – «единообразный адрес ресурса») в IP-адрес. Сейчас мы попробуем рассмотрим эту систему более детально.

Она называется DNS, то есть Domain Name System, система доменных имен. Работой службы DNS в глобальном масштабе управляет ICANN (Internet Corporation for Assigned Names and Numbers, Международная корпорация по присвоенным именам и номерам). Тут господствует принцип той же иерархии, что и при раздаче IP-адресов. ICANN создает домен верхнего уровня и дает региональным регистраторам доменов право присваивать имена более низких уровней в этом домене (начиная со второго) определенным IP-адресам. Что же такое домен? Рассмотрим какой-нибудь адрес сетевого ресурса, например music.yandex.ru. Так вот, это домен третьего уровня. Домен первого уровня – .ru. Домен второго уровня – yandex.ru. Домен некоего уровня интересен тем, что в нем можно разместить несколько доменов более низких уровней, причем тут фантазия ограничена только практическими соображениями, то есть удобством запоминания интернет-адреса.

Итак, для того чтобы выдавать на каждое зарегистрированное в интернете доменное имя соответствующий ему IP-адрес, есть служба DNS. По одноименному с ней протоколу компьютер при вводе URL запрашивает специальный прописанный в его настройках сервер с целью выяснить, к какому IP-адресу обращаться. Сервер DNS ему отвечает, и он может установить соединение. У каждого провайдера есть свой DNS-сервер. Разумеется, он не может держать на своих дисках таблицу соответствия IP-адресам для всех URL в мире. Но для этой благородной и жизненно важной для сети интернет цели есть специальные, очень большие DNS-серверы. Они называются корневыми, и их всего 13 во всем мире. Большинство, кстати, находится в США. Если в кэше DNS-сервера провайдера нет нужной записи, он обращается к серверу более высокого ранга с запросом и добывает ее. Иногда запрос доходит по цепочке и до корневых серверов, и не сказать чтобы редко.

Итак, для выхода в интернет компьютеру необходимо знать IP-адрес DNS-сервера. Провайдер может выдавать его динамически по протоколу DHCP, так же как IP-адрес и некоторые другие настройки, а может просто написать в инструкции в явном виде. Тогда его нужно вбить в подходящее поле настройки сети на роутере (интернет-шлюзе) или конкретном компьютере. Чаще всего провайдер дает адреса двух DNS-серверов, и ввести желательно оба.

Можно легко проверить, все ли в порядке с настройками DNS. Для этого надо обратиться к какому-нибудь ресурсу сначала по имени, а потом по IP-адресу. Например, у yandex.ru IP-адрес такой: 213.180.204.11. И если команда ping yandex.ru выдает ошибку, a ping 213.180.204.11 без проблем осуществляется, значит, что-то не так со службой DNS. Либо настройки неактуальны (например, провайдер поменял адрес сервера DNS), либо с самим этим сервером проблемы.

> **Можно легко проверить, все ли в порядке с настройками DNS. Для этого надо обратиться к какому-нибудь произвольному ресурсу сначала по имени, а потом по IP-адресу.**

Вперед, в большую сеть!

Для того чтобы вывести машину из ЛВС в интернет, нужен маршрутизатор (роутер) или компьютер, играющий роль шлюза. При ручном, а не автоматическом вводе параметров сети необходимо указать на каждой из машин IP-адрес и маску подсети (подробности см. в «Практикуме»), а также адреса DNS-серверов (их надо выяснить у интернет-провайдера). Хотя DNS вообще-то бывает достаточно указать на роутере (шлюзе). Да, и еще надо указать адрес того самого шлюза. Причем задавать надо его внутренний сетевой адрес. В большинстве домашних и малых офисных сетей, где в качестве шлюза задействован роутер, он такой: 192.168.1.1, ну или похожий.

Однако ни слова не было сказано про настройку самого роутера или шлюза на взаимодействие с интернетом. Но это сделано просто потому, что тут разговор короткий: при подключении к конкретной сети провайдер просто инструктирует вас о том, с какими основными настройками нужно выходить в интернет. В зависимости от протокола, по которому осуществляется доступ в сеть, набор может варьироваться. Рассмотрим несколько популярных вариантов.

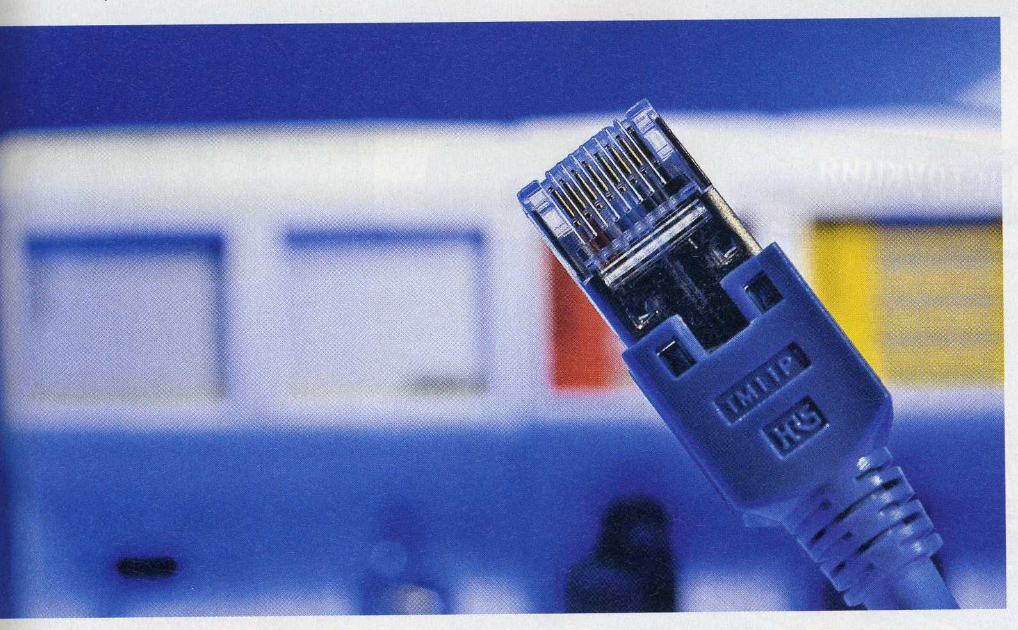
Если доступ предоставлен через Ethernet (или другой протокол поверх него) со статическими IP, выдается IP-адрес, маска подсети, основной шлюз и адреса DNS. Если связь с глобальной сетью устанавливается по протоколу PPPoE, PPTP или другому, требующему ввода логина и пароля, то возможны два варианта. Первый – когда дело ограничивается парой «логин-пароль», а остальное выдается автоматически по специальным протоколам. Второй вариант – когда кроме этого выдают тот же полный набор статических настроек.

Кроме перечисленного выше для корректной работы с внутренними ресурса-

RSS IP-адреса приписываются не собственно компьютерам, а сетевым интерфейсам. Один комп может иметь две или более сетевые карты и работать в нескольких локальных сетях одновременно. У маршрутизаторов всегда два IP-адреса – внутренний и внешний.

ми домовых и районных локальных сетей иногда требуется поправить на шлюзе таблицу статической маршрутизации. Инструкция для этого, опять-таки, добывается у провайдера.

Обратите внимание на то, что все настройки, которые берутся у провайдера, надо применять к WAN-порту роутера, то есть тому интерфейсу сети, который смотрит во внешнюю сеть, а не в вашу собственную локалку! Особенно внимательно за этим надо следить, если настройка ведется не на роутере, а на компе с несколькими сетевыми картами. На всякий случай лучше перед сменой параметров делать скриншоты со старыми их значениями, чтобы потом можно было их вернуть.



О чем боятся спросить

Теперь, когда вы в общих чертах освоились с локальными и глобальными вычислительными сетями на всех уровнях модели DOD, самое время вспомнить некоторые понятия, которые, даром что относятся к теме компьютерных сетей, не были описаны при обсуждении моделей OSI и DOD. И прежде всего это «сервер». Несмотря на то что само это понятие упоминалось в тексте данного материала уже четырнадцать раз, о том, что за ним стоит, не было сказано ни слова. Вообще, как правило, человек, не знающий или неуверенный в том, что такое сервер, предпочитает не спрашивать об этом. Тем более надо объяснить все как можно более четко. Что не так просто. Но я постараюсь.

Существует такая концепция взаимодействия по вычислительной сети: «клиент-сервер». Она сводится к тому, что клиент отправляет серверу запрос, а сервер на него отвечает. То есть клиент заказывает у сервера некую услугу (отсюда название «server», то есть «обслуживающий»). Причем этой услугой может являться что угодно, в зависимости от специализации сервера: IP-адрес в обмен на URL у DNS-сервера, страница сайта в обмен на ее адрес у веб-сервера, файл в обмен на его путь у FTP-сервера. Представили себе?

Теперь самый тонкий момент, сродни психологическим и духовным изысканиям: надо четко определить, кто запрашивает услугу, а кто предоставляет. Строго говоря, и то и другое происходит на уровне программного обеспечения. Например, веб-страницы у веб-сервера запрашивает браузер, а файлы у FTP-сервера – клиент FTP. А программа, отвечающая на эти запросы с того конца канала, и называется собственно сервером. Так что же получается, сервер – это чисто софтовое понятие, просто класс программного обеспечения? Конечно, нет.

Дело тут в том, что востребованные клиентами услуги надо предоставлять бесперебойно, в режиме «24/7». Сеть должна работать постоянно. А для этого компьютеры, на которых крутятся предоставляющие услуги программы, должны быть более надежными, чем обычные клиентские машины. К тому же к популярным сетевым сервисам вроде поисковых машин или онлайн-хранилищ видео и музыки одновременно обращаются со всех концов интернета толпы клиентов. А значит, их мощность должна быть настолько большой, чтобы без проблем выдерживать натиск и не «падать». В связи с этим был выделен отдельный класс надежных, мощных и легко масштабируемых (объединяемых друг с другом для увеличения производительности) вычислительных машин. Их, не мудрствуя лукаво, назвали тоже серверами, а теперь из-за этого такая путаница. Но мы все же разобрались, что к чему.

Осталось добавить, что серверы (в смысле ПО) можно ставить и на обычные персональные компьютеры. Мало того, в состав браузера Opera последних версий входит прелюбопытный многоцелевой сервер Unite с простым в освоении интерфейсом. Если вы еще не «поднимали» серверов, можете начать с него. А можете пойти классической стезей – почитать руководства из Сети и запустить на своем ПК веб-сервер Apache. Что с ним делать дальше – тема, выходящая далеко за рамки этого материала (смайл).

Кроме отношений «клиент-сервер» в сети встречается принцип «равный-равному» (peer-to-peer). При такой схеме каждый ее участник – и клиент, и сервер, то есть и высылает свои запросы, чтобы пользоваться услугами, и откликается на чужие, предоставляя услуги. Так работают файлообменные протоколы BitTorrent и DC, а также знаменитый сервис Skype.

Время закидывать сети

Теперь вы знаете об устройстве сетей достаточно, для того чтобы адекватно воспринять остальные статьи в этом номере (смайл). Мало того, после знакомства с данной статьей вам будет проще управляться с конкретными локальными сетями, и понятнее будут принципы работы глобальной сети. Далее вас ждут более конкретные сведения о сетевом оборудовании, строении сетей, протоколах и прочих нюансах, но общую картину вы уже видите. Не подробную, зато масштабную и иерархически упорядоченную.

Эти знания помогут вам, если вы соберетесь создавать или администрировать сеть. Конечно, их не хватит, и надо будет обязательно прочесть более подробные руководства. Однако будет хотя бы понятно, о чем в них идет речь. Как видите, все устроено максимально просто и красиво – а то, что все сложно выглядит на первый взгляд, это результат в основном огромного масштаба и разнообразия глобальной сети. Основные, базовые принципы и концепции тут, в сущности, нехитрые, и они вполне поддаются освоению. **UP**

RSS Еще IP-адреса имеют Ethernet-интерфейсы таких девайсов, как принтеры и некоторое сетевое оборудование. Если устройство работает на межсетевом уровне DOD, у него есть айпишник. А если на уровне сетевого доступа (как свич или хаб), то нет.

Сетевой ТВ-адаптер Air 7124

Это устройство даст вам возможность просмотра цифровых каналов HDTV на обычном телевизоре без ПК и без проводов. Правда, не стоит забывать о том, что это осуществимо только при заключении договора на поставку соответствующих услуг с одним из интернет-провайдеров. Без такого соглашения найти применение приставке будет крайне сложно.



- **Поддерживаемые форматы видео:** MPEG-2, H.264, VC1, DivX, XviD
- **Интерфейсы:** SCART, HDMI, USB 2.0, Wi-Fi, оптический, Ethernet
- **Габариты:** 253 x 170 x 33 мм
- **Подробности:** www.airties.ru

Сетевой медиаплеер Iconbit HDS52L

Ценность этого медиаплеера определяется тремя вещами. Во-первых, он поддерживает работу с колоссальным числом различных форматов. Во-вторых, устройство оснащено необходимым набором интерфейсов, позволяющим получать мультимедийный контент из Сети. В-третьих, на Iconbit HDS52L установлена очень привлекательная цена.



- **Чипсет:** Realtek RTD1073
- **Поддержка HDD:** 1 x 3,5"
- **Интерфейсы:** HDMI, USB, Ethernet
- **Число поддерживаемых форматов:** 30
- **Габариты:** 55 x 215 x 74 мм
- **Подробности:** www.iconbit.ru

Комплект сетевых адаптеров WD Livewire

Как бы скептически ни относились знающие люди к таким устройствам, мы не можем не признать их полезность при организации домашней сети: мороки с прокладкой проводов не будет. Еще нужно отметить, что оба адаптера имеют по четыре порта Ethernet, поэтому с их помощью можно объединить до восьми ПК или других устройств.



- **Интерфейсы:** Ethernet, HomePlug AV (220 В)
- **Цвет:** черный
- **Габариты:** 32 x 119 x 86 мм
- **Вес:** 190 г
- **Подробности:** www.wdc.com

Маршрутизатор Netgear WNR3500L

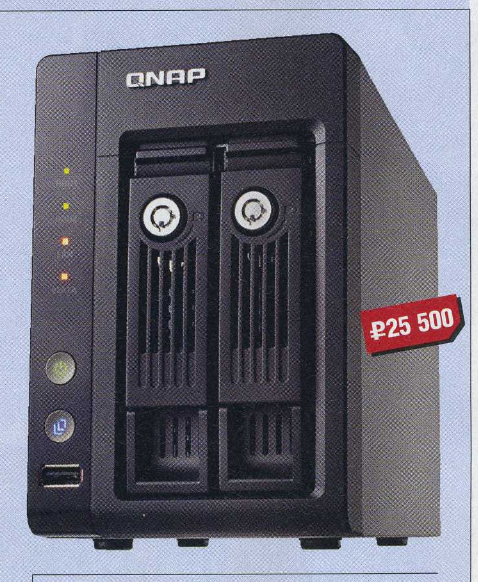
Для домашней сети более продвинутого устройства не найти. Оно оборудовано пятью Ethernet-портами (1 x WAN, 4 x LAN), встроенным модулем 802.11n, а также имеет разъем USB 2.0. Чтобы предотвратить вторжение в организованную беспроводную сеть, администраторы могут воспользоваться протоколами WPA, WPA2-PSK и Push'N'Connect.



- **Интерфейсы:** Ethernet, Wi-Fi, USB
- **Особенности:** Gigabit Ethernet
- **Гарантия:** 2 года
- **Габариты:** 175 x 130 x 35 мм
- **Подробности:** www.netgear.ru

Сетевой накопитель QNAP TS-259 Pro

Для полноценной работы с компьютером потенциальному потребителю нужно будет докупить пару жестких дисков, после чего покопаться в мастере настроек. В нем представлены опции управления дисковыми томами и общими папками, а также подключенными пользователями. Кроме того, можно организовать работу по защищенному каналу HTTPS, настроить две разных подсети, блокировать систему при обнаружении попытки подбора пароля, ограничить доступ по IP-адресам, просмотреть логи операций с файлами и сделать много чего еще. В меню найдется информация о температуре функционирующих винчестеров и скорости вращения вентилятора. Сильной стороной модели стоит считать многообразие выведенных на ее заднюю панель портов, среди которых присутствуют пара разъемов eSATA, два контроллера RJ-45, пять USB-коннекторов и VGA-разъем.



- **Процессор:** Intel Atom D510, 1,6 ГГц
- **Оперативная память:** 1 Гбайт
- **ОС:** Embedded Linux
- **Габариты:** 150 x 102 x 216 мм
- **Подробности:** www.qnap.ru

RSS

Сеть – система связи ПК или компьютерного оборудования. Для передачи данных могут быть использованы различные физические явления – разнообразные виды электрических и световых сигналов или электромагнитного излучения. (Wiki)

Смысл честности

Windows 7 была выпущена осенью 2009 года, почти год назад. Аналитики, особенно те, кому довелось принимать участие в пререлизном тестировании новой ОС, предсказывали ей успех, но то, как публика восприняла «семерку», превзошло ожидания.



Иван Петров
ivanpetrov@upweek.ru
Mood: позитивное
Music: заставка Windows

Достаточно сказать, что к настоящему моменту в мире продано более 240 миллионов копий системы, каждую секунду редмондский гигант продает 8 копий новой ОС, и, по прогнозам аналитиков, меньше чем через год на подавляющем большинстве пользовательских персональных компьютеров мира будет установлена именно Windows 7.



По мнению большинства специалистов, данная система вобрала в себе все лучшее, что было в предыдущих поколениях «форточек». Существует пять различных версий Windows 7, каждая из которых предназначена для своей целевой аудитории, что позволяет любому пользователю выбрать систему, наиболее полно отвечающую его запросам. Они отличаются не только функциональностью – что естественно, но и ценой, поэтому достаточно легко найти себе именно тот вариант, которые по соотношению «стоимость-возможности» подойдет именно вам.

Другой вопрос, что на самом деле в мире установлено значительно больше копий операционной системы Windows 7, чем говорится в официальных отчетах о продажах компании Microsoft. Объясняется это просто: популярность «семерки» достаточно велика, чтобы часть пользователей не стеснялась нарушать законы сразу большого количества стран, устанавливая себе нелицензионные копии и радостно ими пользуясь. Другой вопрос, что эти юзеры зачастую не подозревают, чего себя лишают.

Да, нелицензионная Windows работает нормально. Да, при большом желании можно напрячься, найти лицензионный ключ или утилиту для взлома системы, воспользоваться ею, после чего даже деликатная «семерка» перестает при загрузке напоминать, что владелец данного конкретного компьютера – вор. Но только в этом случае он лишается одной из важнейших функций системы – возможности автоматического обновления, от которой в современном мире зависит довольно таки много вещей.

Ни для кого не секрет, что интернет стал довольно-таки опасным местом. Даже если не брать в расчет вирусы, которые портят жизнь пользователям, так сказать, бескорыстно, искусства ради, остаются зловреды, написанные плохими людьми для решения вполне конкретных задач, к примеру, для того чтобы воровать личные данные пользователей, пароли, номера их кредитных карт или частную переписку – такую как логи аськи.

Подобного рода вредоносные программы появляются каждый день, и единственный способ для вашей Windows вовремя о них узнать – с помощью автоматической системы обновления, которую денно и нощно наполняют оперативными полезностями специалисты компании. Встроенный в систему антивирус – кстати, признанный одним из самых надежных на данный момент, который при этом можно скачать совершенно бесплатно на сайте www.prosto7.ru, – становится практически непреодолимым препятствием для большинства даже совершенно новых опасностей, которыми ежечасно пополняется Сеть.

Поэтому подумайте, получится ли та экономия, на которую принято рассчитывать, пользуясь пиратской системой, или лучше потратить побольше денег сразу, но потом быть уверенным, что за вас ваши деньги не потратит никто.

Ну и программисты Microsoft будут благодарны – они много лет старались, разрабатывая эту систему, а зарплаты они получают в основном благодаря тем, кто компанию не надувает. **UP**

Microsoft – одна из крупнейших транснациональных компаний по производству программного обеспечения. Продукция Microsoft продается более чем в 80 странах мира, программы переведены более чем на 45 языков.

Построение сетей от 0 до 1

Времена, когда лишь умение «уверенно пользоваться ПК» было обязательным, похоже, уходят в прошлое. Сегодня большинство компьютеров объединены в сети, поэтому и общее понимание принципов их функционирования будет полезным для каждого, кто с ними работает.



Konstructor
hard@upweek.ru
Mood: довольный
Music: Bush

Персональный компьютер, не подключенный к сети, представляет собой жалкое зрелище. Не менее постыдное зрелище являют собой и пользователи, перекидывающие друг другу файлы на разнообразных флэшках или, упаси господи, на дискетах. Построение, наладка и поддержание в работоспособном состоянии сети – первостепенная задача любого системного администратора, если, конечно, он не занимается какой-нибудь узкоспециализированной эзотерикой. Его подопечным тоже опасно расслабляться, так как им в этих сетях приходится исполнять свои непосредственные обязанности, для чего могут потребоваться новые навыки и знания.

Статья предназначена в первую очередь для тех, кто в перспективе не против эти сети строить, но пока не обладает не только базовыми знаниями, но и какими-либо ориентирами, указывающими, в каком направлении гуглить. Впрочем, и обычным смертным она тоже может оказаться полезной. Примерно представляя, что к чему, будет гораздо проще объяснить специалисту техподдержки суть проблемы или хотя бы избежать его насмешек и не стать очередным персонажем айтишных баек. Статья не претендует на академичность и глубину, скорее это тот минимум из теории и практики, который позволит быстро поднять небольшую сетку дома или в офисе или хотя бы получить относительно полную картину того, что и зачем бегает по медным проводам, уходящим в коробы или электрические щитки. Ну, и начнем мы, конечно же, с теории, потому что объяснить без нее происходящее на практике практически невозможно (смайл).

Теория и снова теория

Чтобы взаимодействовать между собой, устройства, подключенные к сети, назы-

RSS

Выдачей IP-адресов, управлением корневыми DNS-серверами и регистрацией протоколов и соответствующих им портов занимается некоммерческая организация под названием IANA. Ознакомиться с ее документами можно на сайте iana.org.

ваемые узлами, должны неукоснительно соблюдать немало довольно сложных правил. Эти правила называют сетевыми протоколами, и они регламентируют все действия, совершаемые узлом в сети, и их последовательность. Они отвечают за то, кто может передавать данные и когда, как узлы находят друг друга в сети, сколько данных за один раз они могут передавать, как они узнают, доставлены ли данные или потеряны в процессе пересылки, а если доставлены, то сохранилась ли их целостность или же чей-то коварный стул исказил своим беспощадным колесом первоначальную суть, передавив кабель. За время существования сетей разнообразных протоколов придумали великое множество, но, к счастью, нам понадобится едва ли десяток, да и в эти не имеет смысла глубоко погружаться.

Узлы взаимодействуют на разных уровнях, используя на каждом свой набор протоколов. Принято выделять семь таких уровней, для чего придумана отдельная классификация, именуемая сетевой моделью OSI. Протоколы более низких уровней отвечают за свою строго определенную часть взаимодействия и предоставляют возможность протоколам более высокого уровня не вникать в многочисленные подробности, а сконцентрироваться на решении собственных задач.

Но, прежде чем думать о высоком, нам надо разобраться с более приземленными задачами, а именно хотя бы передать последовательность сигналов по сетевому кабелю. За это отвечают протоколы физического и канального уровней. Они регламентируют, как кодируются и передаются по кабелям или радиоэфиру собственно сигналы и как узлы могут преобразовать их в понятные всем биты. Самым популярным семейством протоколов этого уровня можно считать Ethernet. Именно с его помощью связываются компьютеры в подавляющем большинстве офисов и домов. Если быть точнее, то за стомегабитную проводную сеть отвечает протокол 100BASE-TX, а за гигабитную – 1000BASE-T. К этому же уровню относится и Wi-Fi (802.11a / b / g / n), Bluetooth, ADSL и другие протоколы, связанные непосредственно со средой передачи данных. Мы будем рассматривать только распространенные локальные сети, так что кроме Ethernet и Wi-Fi нам бояться нечего.

Как передавать, мы, допустим, разобрались, теперь надо найти в сети другие компьютеры. У каждого узла в локалке существует несколько различных адресов, предназначенных для протоколов разных уровней. На канальном уровне нам приходится иметь дело с MAC-адресами (Media Access Control – управление доступом к среде).

Эти адреса присваиваются каждому проводному и беспроводному интерфейсу еще на заводе-изготовителе оборудования и теоретически никогда не могут повторяться. MAC-адрес представлен в виде последовательности из шести чисел, записанных в шестнадцатеричной форме – слитно либо разделенных двоеточиями или дефисами, например 00-18-F3-E0-42-E9. В трех первых байтах MAC-адреса закодирован производитель оборудования, в данном случае ASUS, а три последних идентифицируют собственно интерфейс. Зная этот адрес, можно передавать данные в одном сегменте сети напрямую, без каких-либо посредников, но не дальше. Сегмент – это физически обособленная часть сети, как правило, ограниченная маршрутизатором, о роли которого мы поговорим чуть позже. Обычно всю офисную или же квартирную сеть можно считать одним сегментом. А вот крупные домовые сети уже бывают разделены на несколько, и на распространение трафика между ними часто накладываются ограничения.

Чтобы добраться до компьютеров в других сегментах и сетях, применяется протокол под названием IP (Internet Protocol – межсетевой протокол), который работает на более высоком – сетевом – уровне. Существует две разновидности этого протокола, версии 4 и 6, которые обозначаются как IPv4, или просто IP, и IPv6. Нас интересует только IPv4 как более распространенный и простой для изучения. Он работает поверх физического уровня и входит в семейство протоколов TCP/IP. В его понимании все узлы

За списки производителей техники и соответствующие им коды в MAC-адресах отвечает организация IEEE. Этот список может помочь выявить проблемные узлы в сети. Скачать его можно по ссылке standards.ieee.org/regauth/oui/index.shtml.

сети имеют только IP-адреса, а про нижележащий уровень он и знать ничего не знает, равно как и тот о нем. Эти адреса задаются уже непосредственно системными администраторами либо пользователями и должны различаться только в рамках одной подсети. В одном физическом сегменте может существовать сколько угодно IP-подсетей, причем они, как параллельные вселенные, никак не будут друг другу мешать.

В четырехбайтовом IP-адресе содержатся как сведения о принадлежности компьютера к какой-либо сети, так и индивидуальный номер компьютера в ней. Какая часть адреса отвечает за первое, а какая за второе, определяет сетевая маска. IP-адрес и маска 4-й версии записываются в виде четырех чисел, разделенных точкой, например адрес 192.168.1.1 и маска 255.255.255.0. Кроме того, адрес сети часто записывают сразу вместе с маской, например 192.168.1.0/24, что равносильно записи 192.168.1.0 с маской 255.255.255.0. Число после косой черты указывает, что для обозначения адреса сети используется 24 бита, а остальные 8 бит задействуются для адреса машины в сети. Соответственно, число 255 в двоичной записи представляет собой 8 единиц, таким образом, умножив 8 на 3, получаем все те же 24 бита. В одном оставшемся байте, который мы выделили маской для адресации узлов, может быть использовано 256 возможных значений, следовательно, в этой сети может существовать 256 минус 2 возможных IP-адреса. Два вычтенных, 192.168.1.0 и 192.168.1.255, являются адресом подсети и широковещательным адресом. Они имеют особое значение, и назначить их узлу нельзя.

В реальности приходится сталкиваться всего с тремя видами сетей и, соответственно, с тремя масками, а именно 10.0.0.0/8, 172.16.0.0/12 и 192.168.0.0/16. В последнем случае сеть может содержать 65 534 узла, но на практике чаще используется 24-битная маска на 254 узла, позволяющая выделить для личного пользования 256 подсетей для самостоятельного разделения собственной локальной сети на сегменты. Остальные хитрые и нестандартные маски, как правило, выдаются интернет-провайдером, и их достаточно ввести, где попросят, при настройке подключения к интернету.

Так как узлы знают только о своих непосредственных соседях из собственной подсети, чтобы достучаться до удаленных узлов, в том числе и из интернета, используется специальный посредник – маршрутизатор, или, если англицизмы ближе, роутер. Маршрутизатор – это компьютер, который знает, куда отправлять пакеты данных, предназначенные для других сетей. Обычно он просто пересылает все на шлюз по умолчанию, адрес которого выдается провайдером, но при помощи таблиц маршрутизации, в которых содержатся маршруты для разных сетей, можно настроить и более сложные правила пересылки. Именно роутеры стоят на границах IP-подсетей или физических сегментов сетей, объединяя их или, наоборот, фильтруя нежелательный трафик.

Поскольку MAC- и IP-адреса находятся на разных уровнях и никак не связаны между собой, существует отдельный механизм, который сопоставляет эти адреса. Протокол ARP (Address Resolution Protocol – протокол разрешения адресов) поддерживает на каждом узле специальную ARP-таблицу, в которой он записывает, какому физическому MAC-адресу соответствует IP-адрес. Не зная физического адреса получателя, мы не сможем спуститься с сетевого уровня на канальный, чтобы передать наши данные непосредственно по проводам или радиоэфиру. Когда мы обращаемся к узлу, физический адрес которого еще неизвестен, протокол ARP рассылает по всему сегменту сети запрос, имеющий примерно следующий смысл: «А у кого здесь адрес 192.168.1.1?» Если обладатель адреса в сети, он отвечает: «У меня» – в то время как все непричастные молчат. Получив ответ, ARP заносит соответствие в

Узнаем IP- и MAC-адрес, таблицы маршрутизации и ARP

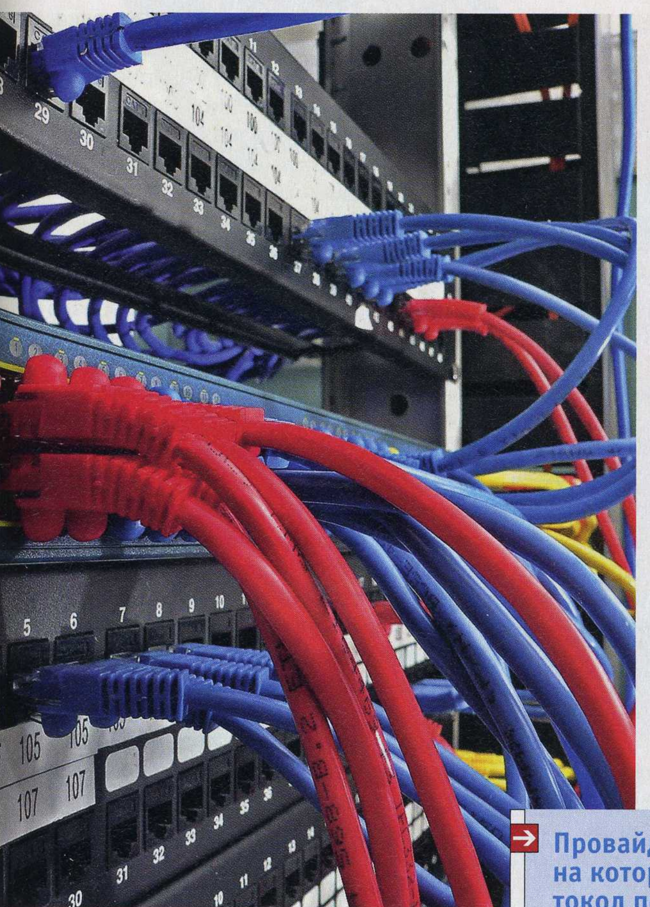
Как известно, лучше один раз увидеть, чем сто раз услышать, поэтому займемся непосредственным наблюдением, знакомясь с тем, как теоретические положения реализуются вживую, на конкретном ПК. Лучше всего проделывать операции на компьютере с Windows XP, так как Vista и «семерка» создают слишком много ненужных виртуальных подключений для собственных нужд. Все команды необходимо вводить в командной строке, наслаждаясь белыми буквами на черном фоне. Сначала выясним IP-адрес. Для этого достаточно набрать команду `ipconfig` без каких-либо ключей. В результате ее выполнения на экран будут выведены основные сведения о существующих сетевых подключениях: IP-адреса, маски, шлюз по умолчанию. Для того чтобы узнать о подключениях побольше, необходимо выполнить команду с ключом `ipconfig /all`. В вывод добавится информация об имени компьютера, MAC-адресах, поддержке DHCP и известных DNS-серверах.

Теперь можно опуститься еще глубже и заглянуть в ARP-таблицу, для чего потребуется ввести команду `arp -a`. На экране появится список из IP-адресов и соответствующих им MAC-адресов. Если обратиться к адресу, которого нет в списке, и выполнить команду еще раз, можно будет увидеть, что он появился. При помощи команды `arp` можно жестко привязывать IP-адрес к физическому, но обычно в этом нет необходимости.

Наконец чтобы взглянуть на таблицу маршрутизации, следует набрать команду `route print`, которая выведет список активных маршрутов. Изначально все маршруты создаются автоматически на основании адреса шлюза по умолчанию, но с помощью этой же команды можно создавать и собственные.

RSS

Разработкой стандартов интернета занимается организация IETF. Они публикуются под названием RFC, сопровожденным порядковым номером стандарта. Их легко найти по ссылке www.ietf.org/rfc.html, но вот осилит хоть один далеко не каждый.



таблицу и хранит его некоторое, довольно непродолжительное, время там, чтобы не засорять сеть ненужными широковещательными запросами.

Разобравшись с адресами, самое время задуматься о том, как передать собственно данные. Хотя протокол IP и может содержать полезную для нас нагрузку и способен пересылать пакеты от одного адресата другому, в каких бы сетях они ни находились, он не имеет ни малейшего представления о том, для кого на машине получателя предназначен пакет. А ведь там может функционировать множество различных сетевых сервисов, и каждый из них согласен работать только со своими пакетами, сформированными и отправленными по своим правилам, а чужие для него не представляют интереса. Чтобы добавить IP ума, поверх него используются еще два протокола, TCP и UDP, которые соответствуют транспортному уровню модели OSI. Если первый заведует адресами отправителей и получателей, то два других располагают информацией о том, какому приложению предназначен тот или иной пакет.

Эти протоколы к понятию адреса добавляют еще и понятие порта. Каждое приложение, заинтересованное в получении данных по известному только ему протоколу, открывает на компьютере порт с определенным номером и ждет, когда кто-то пришлет данные именно на этот порт. Указание порта и подразумевает явным образом, что пакет предназначен приложению, «слушающему» этот порт, и, следовательно, поддерживает протокол, который понимают и приложение-отправитель, и приложение-получатель. Два разных приложения не могут «слушать» один и тот же порт, поэтому в случае такой коллизии кому-то придется или не работать, или использовать другой порт. Во вступительной статье приведен краткий список некоторых стандартных портов. Кроме того, в процессе передачи данных приложения могут по договоренности открывать и использовать другие порты, но не младше 1024-го. Существует стандартизованная таблица с указанием портов и соответствующих им протоколов, и вплоть до 1024-го порта применять их не по назначению считается моветоном. Разумеется, никто не запрещает заставить приложение открыть для подключения любой другой порт, от 1-го до 65 535-го, однако в этом случае отправителю нужно будет точно знать, на какой порт он должен отослать пакеты, чтобы получить ожидаемый результат.

Маршрутизаторы могут блокировать трафик, предназначенный для некоторых портов. Провайдеры часто закрывают 25-й порт, на котором по умолчанию работает протокол передачи почты SMTP, чтобы предотвратить рассылку спама с зараженных машин в сети. Системные администраторы в целях безопасности блокируют для своих пользователей вообще все порты, кроме 80-го.

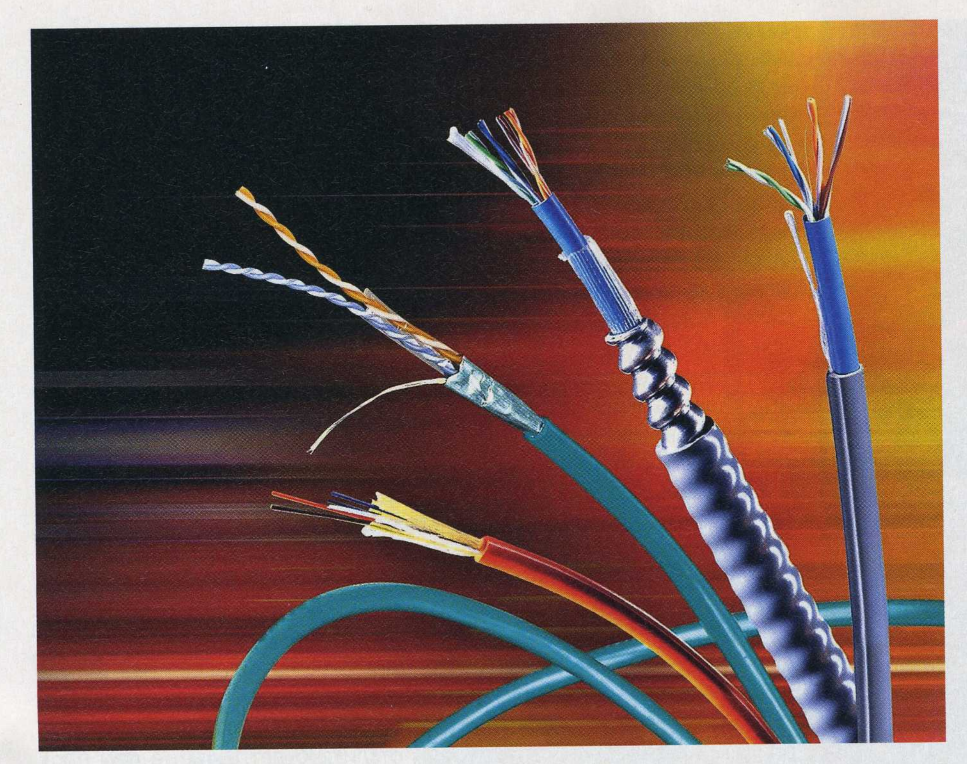
Провайдеры часто закрывают 25-й порт, на котором по умолчанию работает протокол передачи почты SMTP, чтобы предотвратить рассылку спама с зараженных машин в сети.

Хотя и TCP, и UDP оперируют единым понятием порта, протоколы эти совершенно разные и используются для разных нужд. Так, TCP (Transmission Control Protocol – протокол управления передачей), прежде чем начать работу, необходимо установить соединение, то есть убедиться, что получатель в сети и готов к приему данных. Кроме того, он гарантирует получение и целостность данных и самостоятельно обрабатывает ситуации потери некоторых пакетов в сети, автоматически перевысылая их заново. Конечно, все эти возможности требуют ресурсов системы и вносят дополнительные задержки при передаче данных, поэтому протокол используется там, где нельзя потерять ни единого пакета.

В отличие от TCP, протоколу UDP (User Datagram Protocol – протокол пользовательских датаграмм) установка соединения не требуется. Он шлет данные порциями, нисколько не заботясь о том, принимает ли их получатель и доходят ли они до него вообще. Благодаря этому время отклика будет выше, а сам процесс передачи будет меньше нагружать систему, но и никаких гарантий доставки получить не удастся. UDP используется там, где в первую очередь нужны скорость и высокое время отклика, а каждый отдельный пакет особой ценности не имеет. Различные сервисы, передающие голос или видео, а также сетевые игры, как правило, применяют UDP. Даже в случае пропуска нескольких пакетов ничего особо страшного не случится – чуть дернется голос, выпадет кадр или противник в игре вдруг замрет, а потом мгновенно перенесется на пару шагов в сторону.

Разобравшись с передачей данных от одних приложений другим, самое время вспомнить, что в жизни мы обычно имеем дело не с IP-адресами, которые трудно запоминать и вводить, а с более понятными для человека символьными именами. Сопоставлением IP-адресов этим именам занимается отдельная система под названием DNS (Domain Name System – система доменных имен), а имена, соответственно, называются доменными. Эта распределенная система выполняет сходную с ARP функцию, но на более высоком – прикладном – уровне. В отличие от протокола более низкого уровня, DNS не рассылает широковещательных запросов – узел должен

Существует и протокол IPv5, однако он был экспериментальным и не получил никакого распространения. В дальнейшем он превратился в протоколы ST и ST-II, предназначенные для потоковой передачи данных в реальном времени и также массово не применявшиеся.



точно знать, к какому DNS-серверу он должен обратиться за информацией. Сервер, в свою очередь, либо ответит клиенту, если знает, какому адресу соответствует запрошенное имя, либо отправит запрос дальше, пока не найдет сервер, ответственный за запрошенное имя, или пока не выяснит, что такого не существует. Серверы DNS используют 53-й порт, применяя для передачи запросов и получения ответов протокол UDP, ведь в этом случае скорость имеет огромное значение, так как, не зная IP-адреса, нельзя начать передачу данных. Адрес DNS-сервера обычно выдает провайдер, и для отдельной квартиры его более чем достаточно, так как в мелких сетях для разрешения имен применяются более простые средства. В средних и крупных офисных сетях обычно есть один или несколько собственных DNS-серверов, отвечающих за имена, используемые внутри этой сети.

Итак, кое-какой фундамент, без которого немыслимо дальнейшее повествование, заложен. Теперь можно отвлечься от нагромождения абстракций и вернуться в физический мир, чтобы засучить рукава и приступить к прокладке сетей.

Медь и электромагнитные волны

Начиная строить сеть, прежде всего необходимо решить, какую среду передачи данных использовать. Сегодня можно выбирать из стомегабитной или гигабитной кабельных сетей либо беспроводной сети стандарта 802.11g или 802.11n. Все варианты имеют как преимущества, так и недостатки, поэтому надо хорошенько взвесить все за и против.

Новейшие проводные сети обычно значительно быстрее новейших беспроводных, в них ниже задержки сигнала, и они меньше страдают от изменений во внешней среде. С другой стороны, к каждому рабочему месту необходимо подвести кабель и розетку для подключения, которые желательно беречь в целости и сохранности, что удается далеко не всегда. Особенно остро встает проблема в офисах, так как их население мало того что пренебрежительно относится к технике и кабелям, так еще и ужасно любит пересаживаться с места на место. Да и рабочих мест почти гарантированно больше, чем запланированных розеток, что тоже добавляет проблем и подстольного хаоса. Обычно в офисе прокладкой кабельных сетей занимается отдельный подрядчик, и занятие это скорее строительное, а не айтишное, тем не менее иногда приходится самому тянуть недостающее. Если же руководство предлагает накидать проводную сеть самостоятельно, это крайне тревожный знак и серьезный повод задуматься о том, стоит ли и дальше работать в этой организации.

Новейшие проводные сети обычно значительно быстрее новейших беспроводных, в них ниже задержки сигнала, и они меньше страдают от изменений во внешней среде.

Беспроводные сети всех вышеуказанных этих недостатков лишены. Будучи подключенным к беспроводной локалке, можно свободно передвигаться и бесконечно пересаживаться в радиусе ее действия без необходимости внесения каких-либо изменений в конфигурацию. На этом, однако, преимущества заканчиваются, и начинаются недостатки. Задержки в беспроводных сетях всегда выше, поэтому они гораздо меньше подходят для игр. Кроме того, если в случае проводных локалок мы получаем максимальную скорость сети для каждого подключенного устройства, то в беспроводных радиоэфир делится между всеми участниками радиообмена, а вместе с ним делится и скорость. На быстродействие также влияет расстояние до точки доступа, наличие других приборов, например микроволновых печей, телефонов с включенным модулем Bluetooth и даже чужих беспроводных сетей. Бетонные стены с металлической арматурой внутри и металлические двери серьезно уменьшают радиус действия беспроводной сети, поэтому через пару капитальных стен сигнал уже может и не пробиться, что приходится учитывать при внедрении. Беспроводная локалка также может быть менее безопасной, ведь для проникновения в нее не требуется физического доступа и непосредственного присутствия, а подбор секретного ключа – часто лишь дело времени.

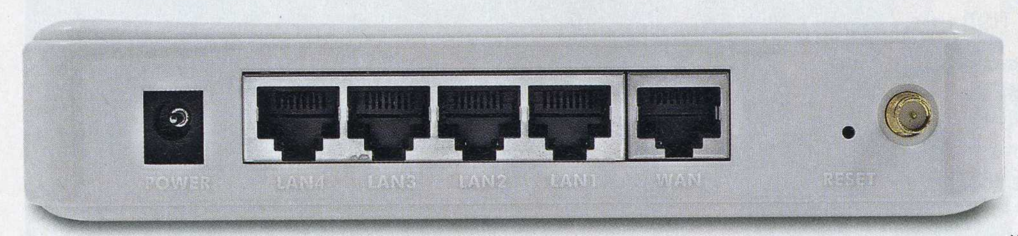
В идеальном случае домашняя или офисная сеть представляет собой комбинацию из проводной и беспроводной, так как каждая способна при необходимости компенсировать недостатки другой. По меди соединяются десктопы, сетевые принтеры и основная часть рабочих ноутбуков. По радио подключаются кочующие или лишенные розеток сотрудники. Серверы и файловые хранилища всегда соединяются между собой проводами, причем желательно гигабитными.

При прокладке кабельных сетей чаще всего используется незащищенный восьмижильный кабель «витая пара», в котором жилы скручены в четыре пары, а те, в свою очередь, скручены между

RSS

Работа утилит ping и tracert основывается на специальном протоколе ICMP (Internet Control Message Protocol – межсетевой протокол управляющих сообщений). Он используется для передачи сообщений о возникающих в сети ошибках и неполадках.

собой для уменьшения воздействия помех на сигнал. Он обозначается аббревиатурой UTP (Unshielded Twisted Pair – неэкранированная витая пара). Кабелям присваиваются категории, определяющие максимальную скорость передачи данных. Для стомегабитной сети используется кабель 5-й категории, а для гигабитной – категории 5е или 6. При монтаже витую пару ни в коем случае нельзя прибивать гвоздями, скобами или иными металлическими крепежами. Лучше использовать пластиковые стяжки на самоклеющихся площадках либо пластиковые коробы. Кабель также нельзя слишком сильно изгибать и перекручивать или прокладывать под прямым углом, подобно телефонному, так как все это может вызвать снижение качества сигнала. Длина провода не должна превышать 100 м. Старайтесь прокладывать кабель так, чтобы он не был натянут, по нему никто не ходил и не ездил на стульях. Спинки стульев представляют особую опасность, так как с их помощью хрупкие и нежные барышни не только со временем перемалывают шнур, но и выламывают розетку, к которой он подключен.



Конечные Ethernet-устройства соединяются с кабелями при помощи прозрачных коннекторов, которые принято называть RJ45. Это название хоть и не соответствует официальному наименованию 8P8C, но в данном случае лучше не умничать, иначе тебя могут просто понять неправильно. На коннекторах имеется ключ в виде торчащего ярлычка, который фиксирует их внутри порта. Чтобы извлечь штекер, необходимо нажать на этот язычок. Встречаются такие варианты, в которых ключ изогнут так, чтобы не торчать и не цепляться за что попало при протягивании. Лучше всего искать именно такие, так как они здорово облегчают жизнь.

В большинстве случаев желательно использовать шнуры с уже установленными заводским способом коннекторами, их длина чаще всего бывает от 0,5 до 5 м. Если же требуется длиннее, придется устанавливать соединитель самостоятельно. Этот процесс называется обжимкой и выполняется при помощи специального инструмента, кримпера, который также называют обжимными клещами или просто обжимкой. При этом лучше не экономить и сразу купить достойное оборудование, а не дешевое китайское «поделие» из бутика дядюшки Ляо, не попадающие на ножи, обрезающее пары вместе с оболочкой или калечащее штекер. В экстремальных случаях можно воспользоваться плоской отверткой и плоскогубцами, но делать это надо крайне аккуратно.

Сам процесс достаточно прост, главное – соблюсти последовательность, в которой жилы должны располагаться внутри коннектора, но, так как они всегда выкрашены в одинаковые цвета, сделать это несложно. Итак, если повернуть соединитель контактами-ножами к себе, а ключом от себя, то последовательность такова: бело-оранжевый, оранжевый, бело-зеленый, голубой, бело-голубой, зеленый, бело-коричневый, коричневый. Важно запомнить, что белые обязательно чередуются с одноцветными, но если вдруг вылетело из головы, всегда можно найти заводской штекер и быстро вспомнить последовательность. После обжима стоит осмотреть результат и убедиться, что все ножи вошли в жилы, что жилы не перепутались и не вывалились. Имеет смысл обзавестись специальным электронным тестером, автоматически прозванивающим кабель и выявляющим битые пары. В случае со стомегабитной сетью можно пренебречь качеством обжимки коричневых и голубых пар, но в гигабитной все должно быть идеально. Кабели 6-й категории оснащены полиэтиленовым сердечником, поэтому их обжимать сложнее. В офисном хозяйстве всегда должны быть запасные коннекторы, обжимка, пара десятков метров кабеля и тестер, их надо требовать с начальства в первую очередь. Для дома покупать все это не стоит, лучше позаимствовать у ИТ-специалистов на работе или даже попросить их помощи по дружбе или же за конфетно-шоколадную и прочую мзду.

После того как кабельная сеть выстроена, необходимо соединить все узлы между собой. Для этого используется специальное устройство, коммутатор, также известное как свич. Дома лучше с самого начала отбросить все сомнения и поставить гигабитный коммутатор на пять или, предпочтительнее, сразу на восемь портов. В офисе же пользователям имеет смысл выделить стомегабитные свичи, а через гигабит-



RSS

В маленьких сетях вместо DNS для разрешения имен используется протокол NetBIOS, известный также как NBT. С его помощью узлы определяют, кто из них хранит список с именами, и автоматически их регистрируют. Имена в сетевом окружении и есть имена NetBIOS.

Основы устранения неполадок в сети

В случае возникновения каких-либо проблем в сети жизненно необходимо уметь их оперативно выявлять и решать. Прежде всего надо проверить связь, для чего ввести ping и IP-адрес или имя проблемного узла либо же адрес общеизвестного сетевого ресурса для определения работоспособности интернета, например ping ya.ru или ping 8.8.8.8. Команда покажет, есть ли ответ от интересующего узла и каковы задержки. В локальной сети они не должны превышать 10 мс, а пакеты не должны теряться вовсе. В беспроводной возможны различные значения в зависимости от мощности сигнала, и даже пропажа некоторых пакетов – обычное явление: в интернете задержки могут доходить до тысяч миллисекунд, а пакеты периодически теряться, что может указывать на проблемы у провайдера.

Если узел в интернете не пингуется, стоит выяснить, чьи это проблемы, провайдера или собственного маршрутизатора. Для этого используется команда tracert с адресом проблемного узла. Она показывает, через какие промежуточные узлы прошли запросы. Если ответа нет даже от шлюза по умолчанию, то проблема в локальной сети. Если пакет проходит пару шлюзов, а потом «умирает», проблема, скорее всего, у провайдера, ну а если ему не хватает буквально одного «прыжка» до интересующего узла, значит, проблемы у хозяев этого узла.

Иногда встречаются проблемы и с DNS-серверами. Для их проверки используется команда nslookup, после которой указывается проблемное доменное имя. Если все в порядке, утилита выдаст IP-адреса, соответствующие этому имени, а если нет, то сообщит о том, что ответ не получен. В этом случае можно попробовать попинговать провайдерский DNS и в случае ошибок смело звонить и негодовать.

ные соединить между собой серверы, файловые хранилища и менее скоростные коммутаторы. Не стоит соединять свичи последовательно, так как это увеличит задержки. Лучше назначить один из них, желательно самый дорогой и мощный, центральным и все остальные соединять только через него. Ни в коем случае нельзя допускать колец при подключении, законнектив, например, первый свич ко второму, второй к третьему, а третий снова к первому. Это приведет к неработоспособности всей сети, а отыскать источник проблемы может быть не так просто. В идеале все соединительные кабели должны быть подписаны, но в реальности часто бывает не до того. Тем не менее надо обязательно подписать хотя бы кабели, идущие к серверам, коммутаторам и другим активным сетевым устройствам. В офисе также обязательно стребовать с подрядчика либо с предшественника схему разводки сети, на которой обозначены все розетки с номерами и их расположение на плане, – в противном случае жизнь все чаще будет казаться мучительной и безрадостной, причем чем больше площадь помещений, тем глубже будет погружение в депрессию.

С беспроводными сетями веселья гораздо меньше. Компьютеры подключаются к ним при помощи точек беспроводного доступа (AP – access point), для которых важно выбрать приличное место. Главное – в процессе не забыть, что точка хоть и беспроводная, но ей понадобится питание, а также кабель для подключения к проводной сети. Не стоит запихивать коробочку с антеннами в непролазную тьму, так как они иногда зависают, и исправить положение можно лишь классическим методом «выключить и включить». Оставлять точку валяющейся под ногами тоже нежелательно, лучше, чтобы она не бросалась никому в глаза, иначе у особо параноидальных сотрудников могут возникнуть опасения насчет облучения или проявиться излишнее любопытство. Прятать точку за металлическим сейфом или дверью, а также холодильником, компьютером либо, боже упаси, микроволновкой – очень плохая идея, сигнал по мере удаления от источника и без их помощи гаснет быстрее, чем этого бы хотелось. Если одной точкой планируется обслуживать сразу несколько кабинетов, необходимо расположить ее так, чтобы количество стен, через которые проходит сигнал, было минимальным, а при наличии капитальных стен следует убедиться в том, что мощность сигнала за ними достаточна.

Сегодня распространены локальные беспроводные сети двух стандартов: 802.11g и 802.11n. В первом случае максимальная пропускная способность составляет 54 Мбит/с, из которых реально можно достичь 20 Мбит/с с радиусом покрытия до 40 м внутри помещения. Во втором случае можно получить от 80 до 160 реальных мегабит в секунду в зависимости от используемого диапазона с покрытием в 70 м. Имеет смысл покупать точку стандарта 802.11n, но важно помнить, что такие карточки до сих пор устанавливаются далеко не во все ноутбуки, а в смешанном режиме эти точки работают медленнее.

После того как точка установлена, необходимо провести ее настройку, сменить администраторский пароль, дать осмысленное название беспроводной сети (SSID) и при необходимости запаролить и зашифровать ее от посторонних при помощи секретного термоядерного ключа и WPA2. Держать или нет домашнюю беспроводную сеть открытой – вопрос дискуссионный. Лично я никогда не раздавал халявы, но вовсе не потому, что я такой патологически жадный. Просто за неосмотрительные действия в сети какого-нибудь анонима отвечать, скорее всего, придется тому, на чье имя оформлен контракт с провайдером, а уж способов серьезно и наказуемо начудить в интернетах сегодня найдется предостаточно.

На этом с медью и эфиром можно закончить, помыть руки и с серьезным видом усесться за клавиатуру – потому что далее речь пойдет о программной части сети.

Софт и конфигурации

Во главе современной сети, как домашней, так и офисной, как правило, стоит девайс, раздающий страждущим интернет. И это вовсе не преувеличение. В сети может сломаться принтер, упасть целый сервер, пару часов не ходить почта, и существует немалая вероятность того, что вам никто и слова не скажет, разве что уж совсем припечет; но, как только у народа асечный цветочек поменяет свой цвет с зеленого на красный, можно ждать шквала звонков, сметающего все на своем пути. За интер-

IP-адрес 8.8.8.8 – это общедоступный DNS-сервер от компании Google. С его помощью можно проверять работоспособность DNS либо увеличить скорость разрешения имен, если провайдерский сервер не справляется с нагрузкой.

нет отвечает маршрутизатор, который вовсе не обязательно должен быть каким-то специальным устройством. Им может выступать и обычный компьютер с Windows XP и двумя сетевыми картами, одна из которых будет видеть локальную сеть, а вторая – глобальную.

Над специальной железкой обычно никаких хитрых манипуляций производить не надо, так как она изначально предназначена для того, чтобы перегонять трафик с одного конца на другой. Порт, к которому подключается кабель от провайдера, обозначается WAN (Wide Area Network – глобальная вычислительная сеть), один или несколько портов, «смотрящих» в локальную сеть, именуются LAN (Local Area Network). Конфигурирование домашних и даже многих профессиональных коробочек осуществляется через веб-интерфейс, для чего к устройству необходимо подключиться и ввести предустановленные изготовителем административные логин и пароль. Ими чаще всего являются admin и admin, но бывают и исключения. Подключаться можно либо при помощи специальной комплектной утилиты, которая автоматически отыщет в сети маршрутизатор, либо вручную, введя в браузере его IP-адрес. Обычно это 192.168.0.1 или 192.168.1.1. В реальных сетях первый адрес ради удобства так и остается закрепленным за маршрутизатором.

Настроить подключение к интернету довольно просто, обычно достаточно внимательно прочитать инструкцию от провайдера. При выделенке вариантов не так много. Если провайдер выдал фиксированный IP-адрес, маску и адрес шлюза по умолчанию, то мы выбираем статическую настройку и вручную вводим все эти значения на вкладке WAN. Некоторые поставщики интернета «статику» не используют и выдают настройки автоматически по протоколу DHCP, о котором мы поговорим чуть позже. В этом случае провайдер привязывает настройки к MAC-адресу того компьютера, который подключал специалист, после того как протянул кабель. Так как обычно они проделывают это с настольными ПК, то роутер, у которого явно другой MAC-адрес, никаких настроек не получит либо получит неверные. Для этого во всех современных маршрутизаторах существует возможность подделки физического адреса, часто даже в автоматическом режиме, когда в качестве MAC для WAN-порта просто берется MAC компьютера, с которого осуществляется настройка. Наконец, третий вариант – соединение через VPN или PPPoE. В этом случае маршрутизатор получает по DHCP любой IP-адрес, а провайдер в качестве настроек выдает логин, пароль и адрес VPN-сервера, которые, опять же, нужно ввести на вкладке WAN, выбрав вместо статической конфигурации подключение по PPPoE. При таком коннекте часто всплывают различные несовместимости, поэтому перед подключением лучше заранее выяснить, какие устройства нормально работают с выбранным провайдером, прошерстив форумы и почитав отклики реальных страдальцев.

При ADSL-подключении по телефонным линиям провайдер старается всучить уже настроенный по всем правилам модем, и порой лучше этим не пренебрегать. Тем не менее можно все настроить и самостоятельно – достаточно найти в договоре или на сайте поставщика интернета настройки для подключения и снова убедиться, что провайдер готов работать с уже имеющимся в доме или офисе ADSL-оборудованием.

В крупных или относительно удаленных офисных центрах провайдер может подводить интернет при помощи оптического волокна, подключенного к его собственному оборудованию. Волокно – вещь очень нежная и хрупкая, поэтому ни в коем случае нельзя его сильно перегибать или протягивать с усилием. Иногда для подключения оптоволокна к собственной сети может понадобиться преобразователь среды, или медиаконвертор. Это небольшая коробочка с двумя портами, оптическим и обычным RJ45, которая чем называется, то и делает – преобразовывает свет, поступающий по волокну, в электромагнитные волны и обратно. Чаще всего конвертор выдает провайдер, но бывают и неприятные исключения. В любом случае подключение таким способом в настройке будет аналогичным выделенному на витой паре.

Относительно того, использовать ли в качестве основы всего интернет-центр «все-в-одном» или же покупать отдельно точку, роутер и свич, можно спорить. В крупном офисе вариантов нет, все будет раздельным в любом случае, а вот дома или в небольшом офисном помещении можно подумать. Интернет-центр стоит недешево, и если он умрет, то погаснет и интернет, и внутренняя, и беспроводная сети, да и, чтобы восполнить утрату, придется выложить полную стоимость всей железки. Не во всех гибридных устройствах имеются и гигабитные порты. С другой стороны, специализированные девайсы, будучи дешевле центра по отдельности, все вместе стоят дороже и занимают в три раза больше розеток. Однако смерть любого из них обойдется дешевле как в плане стресса, так и в финансовом. Также в этом случае возможно делать постепенный апгрейд: заменить точку доступа с g на n или изменить способ подключения, прикупив другой роутер. Как всегда, стоит самостоятельно взвесить все достоинства и недостатки и решить лично для себя, что перевешивает.

Доступ в интернет в современных сетях осуществляется при посредстве технологии NAT (Network Address Translation – трансляция сетевых адресов). С ее помощью, имея лишь один интернетовский IP-адрес, полученный от про-

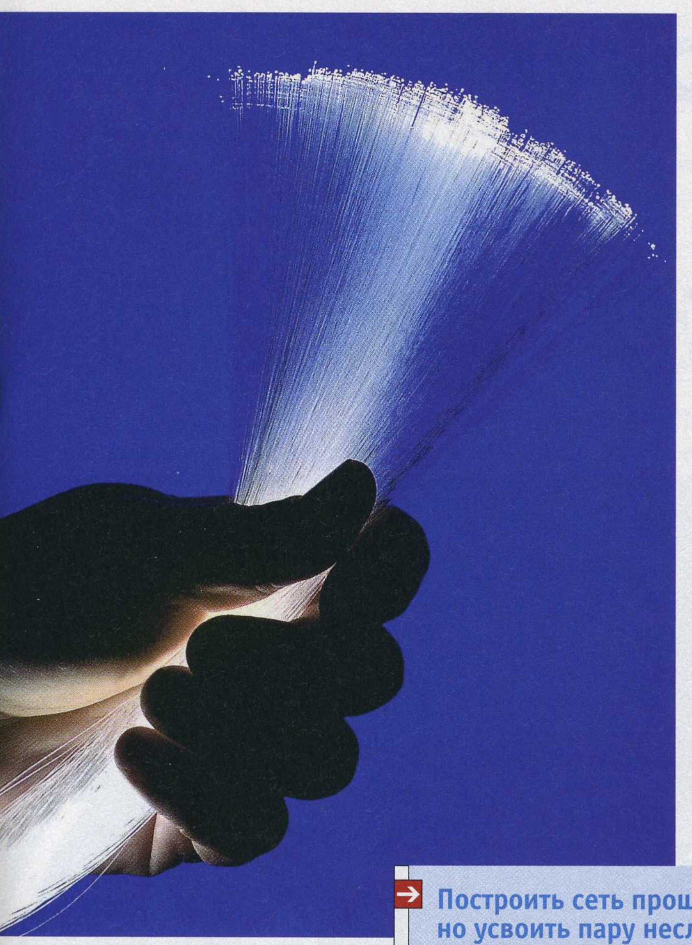
Маршрутизатор **своими** руками

Случается так, что в доме имеется лишь один компьютер, напрямую подключенный к интернету, и при появлении второго претендента на трафик раскошеливаться на дополнительный девайс очень не хочется. К счастью, в маршрутизаторе нет ничего настолько волшебного, с чем бы не справился софт, поэтому назначить им можно обычный компьютер. Для этого необходимо воспользоваться встроенным в Windows средством «Общий доступ подключения к интернету» (ICS – Internet Connection Sharing). Аккуратный мастер шаг за шагом превратит машину в роутер, настроит DHCP, NAT и перенаправление портов. Для того чтобы все заработало, придется включить встроенный в Windows брандмауэр, так как разделяемый интернет и файрволл – по сути одна служба.

Минусы у данного подхода тоже есть – куда же без них. Надо держать шумный и жрущий немало электричества компьютер постоянно включенным, чтобы все остальные могли получать доступ в интернет, – маршрутизаторы же потребляют гораздо меньше электричества и абсолютно бесшумны. Вдобавок вылазки соседних ПК во Всемирную паутину могут негативно сказываться на производительности основной машины. К тому же отдельный маршрутизатор также обладает гораздо более развесистыми настройками, чем не сможет похвастаться встроенное в Windows решение.

RSS

Эндрю Таненбаум (Andrew Tanenbaum) – профессор Амстердамского свободного университета, возглавляет группу разработчиков компьютерных систем, доктор наук. Известен как автор свободной ОС Minix и фундаментальных книг по компьютерным наукам.



> **Построить сеть проще простого. Достаточно усвоить пару несложных понятий, накидать по углам проводов, соединить все через пару свичей да воткнуть в роутер, чтобы все интернетило (смайл).**

вайдера (а в домашних сетях не имея в своем непосредственном распоряжении и его), можно вывести в глобальную сеть большое количество компьютеров, и никто ничего не заметит. На практике это означает, что в своей локалке мы можем быть трижды хозяевами, но интернет ничего этого не увидит, и компьютеры в IP-сетях с приватными адресами будут недоступны извне. Маршрутизатор выступает как непробиваемый файрволл, поскольку он не маршрутизирует пакеты снаружи внутрь. Иногда все же надо иметь такую возможность, например, чтобы выставить наружу свой FTP- или веб-сервер, и для этого есть решение. С помощью функции перенаправления портов (port forwarding) виртуального сервера (virtual server) или статической трансляции адресов (SAT) – у разных производителей она называется по-разному – можно сказать маршрутизатору, чтобы он прикинулся сервером и открыл некоторые порты. В этом случае все пакеты, полученные на указанные порты, роутер будет перенаправлять на некий узел внутри сети, который и является настоящим сервером. Для клиентского и серверного приложений все абсолютно прозрачно, а весь обман осуществляется маршрутизатором. Естественно, трафик с одного порта можно перенаправлять только на один сервер, и повесить десяток разных веб-серверов на один 80-й порт не получится.

Разобравшись с интернетом, стоит наконец навести порядок и в собственной сети, в частности решить, каким образом назначать IP-адреса. Варианта два: можно вручную прописать адреса в настройках подключений либо использовать автоматическую настройку по протоколу DHCP (Dynamic Host Configuration Protocol – протокол динамической конфигурации узла). Первый вариант может сгодиться для домашней сети без ноутбуков и беспроводных гаджетов и уже почти неприемлем для сколь-нибудь большого офиса, поэтому на практике используются оба, так как они взаимно дополняют друг друга. Принцип работы протокола прост: каждый раз, когда узел перезагружается, он отправляет в сеть широковещательный запрос с просьбой выдать ему IP-адрес. При этом ответить ему может любой DHCP-сервер, поэтому в одной IP-подсети он может быть только один, иначе возникнут неминуемые конфликты. Выдав узлу IP-адрес и попутно сообщив ему остальные необходимые настройки, такие как адрес DNS-сервера и адрес шлюза по умолчанию, DHCP-сервер помечает, что адрес занят, и следующему узлу выдает уже другой. В мелких сетях с этой работой может справиться маршрутизатор или беспроводная точка доступа, но в крупных имеется отдельный DHCP-сервер, обладающий значительно большими возможностями и более удобный в обслуживании.

Несмотря на удобства, предоставляемые протоколом DHCP, серверы, файловые хранилища и принтеры принято снабжать статическими адресами во избежание неожиданностей. Серверам назначаются айпишники из начала адресного пространства, например от 10 до 30 в зависимости от количества, а принтерам – все адреса после 200-го и выше, опять же в зависимости от их количества. Всем пользовательским машинам лучше выдавать адреса исключительно через DHCP-сервер, даже если требуется, чтобы чей-то айпишник был неизменным. Для этого на DHCP-сервере создается исключение, в котором явно обозначается, что конкретный IP-адрес можно выдавать только узлу с указанным MAC-адресом и никому более. Исключения поддерживаются и устройствами, и отдельно стоящими серверами.

Выдав всем IP-адреса и выпустив скучающих людей в сеть, начальный этап настройки локалки можно считать завершенным. Далее можно заводить пользователей, устанавливать серверный софт, настраивать сетевые принтеры и правильно выставлять кактусы на столе главбуха, чтобы они поглощали как можно больше зловещего излучения, идущего от ЖК-монитора.

Напоследок

Как выяснилось, построить сеть проще простого. Достаточно усвоить пару несложных понятий, накидать по углам проводов, соединить все через пару свичей да воткнуть в роутер, чтобы все интернетило. Шутка это или нет, каждый волен решать в меру глубины собственных познаний (смайл). Естественно, вместить в одну коротенькую статью весь материал, накопленный человечеством, невозможно, но рассказанного должно вполне хватить, для того чтобы начать и затем продолжить изучение вопроса самостоятельно. Практические советы помогут не наступить на грабли в самых очевидных местах. Безусловно, многие технические подробности были опущены, а некоторые основополагающие понятия даже не были упомянуты, но журнал и не претендует на то, чтобы полностью заменить книгу, да это и невозможно. Например, фундаментальный труд Эндрю Таненбаума «Компьютерные сети» – это томик толщиной в 992 страницы, без четверти подшивка UPgrade за полгода. **UP**

Некоторое время назад слово «интернет» было принято по правилам языка писать с большой буквы как имя собственное. Официально с тех пор ничего не изменилось, но де-факто оно стало именем нарицательным, в связи с чем в литературе пишется со строчной буквы.

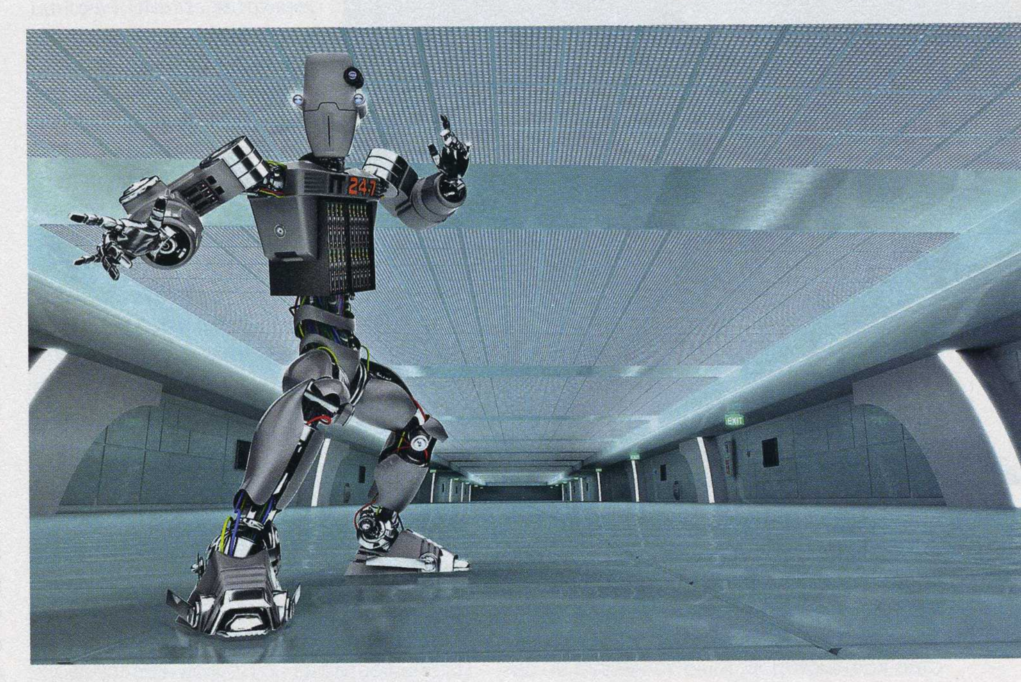
Выбор сетевого оборудования

Как пишут на Lurkmore.ru, «в эту статью нужно добавить как можно больше хорошего сетевого оборудования». Так и поступим. Рассмотрим роутеры и свичи для домашних и малых офисных сетей, беспроводные устройства, NAS'ы и даже сетевые медиаплееры.



DjFedos
hard@upweek.ru
Mood: sleepy now
Music: David Bowie

Не забудем также кабельные тестеры и, конечно, обжимные клещи – это не совсем сетевое оборудование, но ведь локалку надо как-то монтировать, и тут эти нехитрые приспособления придутся как нельзя кстати. Но начать надо с самого основного.



С чего начинаются сети?

А именно с самой тривиальной аппаратной составляющей – кабеля Ethernet. В современных сетях используется чаще всего обычная незащищенная витая пара усовершенствованной пятой категории (UTP CAT5e). Такой кабель обладает полосой пропускания 125 МГц и содержит четыре витые пары. За счет этого при использовании всех четырех пар он способен обеспечивать скорость 1 Гбит/с на расстоянии 100 м, а по двум витым парам может передавать на такое же расстояние по 100 Мбит данных за секунду.

Такой кабель оканчивается с обеих сторон стандартными коннекторами. Обычно их называют RJ 45, хотя на самом деле это распространенная ошибка, и их надо именовать 8P8C. Для того чтобы кабель с гарантией заработал правильно сразу после обжатия коннекторов, нужно соблюсти схему подключения. Существуют два стандарта, по которым обжимают штепсели UTP: A и B. Стандарт A используется редко, а стандарт B – почти всегда. Порядок проводов слева направо, если смотреть на контакты, держа штепсель «брюшком» вверх: бело-оранжевый, оранжевый, бело-зеленый, синий, бело-синий, зеленый, бело-коричневый, коричневый. (Он уже приводился в практикуме по сетям, но повторить не грех.) Раньше в некоторых случаях (скажем, при связи двух сетевых карт напрямую) применялась схема перекрестного обжима (на одном конце кабеля – каноническая схема B, а на другом зеленый провод меняется местами с оранжевым, а бело-зеленый – с бело-оранжевым). На данный момент она почти никогда не требуется, так что можете не заучивать порядок цветов. При создании сети с пропускной способностью до 100 Мбит/с можно использовать четырехжильный кабель. В этом случае задействуются контакты коннектора под номерами 1, 2, 3 и 6. Цвета проводов остаются те же – бело-оранжевый, оранжевый, бело-зеленый, а затем зеленый.

Имейте в виду: если обжать два коннектора Ethernet на концах кабеля одинаково, но не по стандарту, сигнал будет проходить по нему плохо либо не пройдет вообще. Это объясняется тем, что пары проводов сделаны витыми специально, с подобранным шагом скрутки, чтобы минимизировать электромагнитные помехи. Если сигнал идет не по одной «косичке», а по двум проводам из разных пар, схема уже не работает и не спасает от помех. Поэтому всегда обжимайте штепсели витой пары по стандарту B.

Выбирать кабель в магазине сетевого оборудования можно, посмотрев в интернете отзывы пользователей. На мой вкус, хороши кабели с цельными медными жилами (а еще бывают, например, с алюминиевыми). Бухта витой пары длиной 305 м стоит от 1500 до 2000 руб., более дешевые варианты надо тянуть как можно аккуратней, так как их легко повредить. Более дорогие, соответственно, отличаются лучшей надежностью. Конечно, необязательно брать сразу бухту кабеля, можно купить нужное количество метров, хотя тогда провод обойдется вам несколько дороже. Коннекторы стоят порядка 2,5-3 руб. за штуку, иногда дороже. Обжимные клещи обойдутся вам ми-

RSS: На внешнюю оболочку витой пары нанесены различные метки. Самые полезные – это метровые отметки. С их помощью можно точно отмерить кусок нужной длины, не пользуясь рулеткой и линейкой, что иногда пугает непосвященных (смайл).

нимум в 300 руб., впрочем, есть и более дорогие и удобные варианты – выбирайте на свой вкус.

Последнее, что вам может понадобиться для монтажа ЛВС, – это кабельный тестер. Самая простая модель стоит от 260 до 300 руб., и ее возможностей вам, скорее всего, хватит.

Куда вести витую пару?

Теперь самое время рассмотреть роутеры – ведь вряд ли вы создаете ЛВС без выхода в интернет, верно? А обеспечить его на данный момент проще всего именно с помощью простого «домашне-офисного» маршрутизатора. Не далее как несколько месяцев назад в нашем журнале (#28 (480)) сравнивались 15 популярных моделей этих устройств. Поэтому здесь рассмотрим лишь еще парочку из числа тех, что не попали в тот обзор.

ZyXEL NBG318S EE

Первый из них – универсальный и популярный девайс, выпущенный хорошо известной компанией ZyXEL. Модель называется NBG318S EE, мы упоминали о ней и в «Большом тесте», и в отдельном материале. С точки зрения дизайна устройство не особенно примечательно: типовой белый корпус, внешняя антенна. Однако кто покупает роутер красоты ради? На покрытие вайфаем среднестатистической городской квартиры мощности сигнала хватает, интернеты практически от всех существующих провайдеров весело раздаются. «318-й», в отличие от более дорогих вариантов, не поддерживает Wi-Fi версии n, ограничиваясь ревизией g, и не имеет поддержки гигабитного Ethernet, однако многим это и не нужно.

Главное его преимущество – мощная встроеннная операционная система ZyNOS, обеспечивающая надежное подключение по любым протоколам и беспроблемную одновременную работу различных служб. А еще у него есть встроенный адаптер HomePlug AV, предназначенный для передачи данных через электрические сети.

AirTies Air 4240

Данная недорогая модель сочетает в себе функции четырехпортового роутера и точки доступа, способной обеспечить подведомственное помещение интернетом со скоростью до 54 Мбит/с (802.11b / g).

Достаточно интересной для бюджетного, в общем-то, девайса является возможность его использования в качестве репитера, то есть устройства, которое увеличивает зону покрытия беспроводной сети. С этой целью в AirTies Air 4240 реализована технология AirTies Mesh. Достаточно разместить девайс в зоне покрытия существующей беспроводной сети и активировать режим репитера, и проблемы с плохим сигналом вас больше беспокоить не будут.

Что немаловажно, на все свои устройства компания AirTies предоставляет три года гарантии.

Netgear WNR3500L

Еще один девайс в нашей сегодняшней подборке произведен фирмой Netgear. Роутер этот дружит с последней ревизией Wi-Fi, оснащен мощным процессором и гигабитными портами Ethernet.

WNR3500L позиционируется как устройство для энтузиастов-линуксоидов, и изготовитель прямо-таки склоняет пользователей к установке альтернативных прошивок. Впрочем, и штатная, хоть и имеет немного архаичный веб-интерфейс, работает хорошо. Производительность начинки позволяет роутеру гнать данные как из Всемирной сети, так и в пределах своей уютной локалки весьма широким потоком. Устройство рекомендуется прежде всего тем, кому нужна большая скорость ЛВС.

Однако ключевую характеристику роутера производители, увы, никогда не приводят, прежде всего из-за неоднозначности ее определения. В самом деле, что такое стабильность работы? Величина, обратная числу потерь связи с интернетом в неделю? И даже если ввести определение, ни один производитель эту цифру не укажет – себе дороже. Поэтому, выбрав маршрутизатор по совокупности технических характеристик (скорость сетевых интерфейсов, поддерживаемые протоколы связи с глобальной сетью, дополнительные возможности), прочтите какой-нибудь его обзор и отзывы владельцев, чтобы узнать, насколько часто аппарат требует перезагрузки. Если говорить о WNR3500L, то со стабильностью у него все в порядке. И кстати,

Таблица 1. Технические характеристики роутеров

	ZyXEL NBG318S EE	AirTies Air 4240	Netgear WNR3500L
Цена, руб.	3900	1650	4000
Количество портов LAN	3	4	4
Беспроводные сети	Wi-Fi 802.11g	Wi-Fi 802.11g	Wi-Fi 802.11n
Протоколы Internet	Ethernet (Dynamic / Static IP), PPPoE, PPTP, L2TP	Ethernet (Dynamic / Static IP), PPPoE	Ethernet (Dynamic / Static IP), PPPoE, PPTP, L2TP
Дополнительно	интегрированный адаптер HomePlug AV	-	WPS
Габариты, мм	162 x 40 x 117	179 x 33 x 125	130 x 175 x 35
Подробности	www.zyxel.ru	www.airties.com	www.netgear.ru

Таблица 2. Технические характеристики свичей

	ASUS GigaX 1005	ASUS GX-D1051	Linksys SD208	Cisco Catalyst 2960-24TT
Цена, руб.	500	1600	1800	25 600
Количество портов	5	5	8	24
Скорость	до 100 Мбит/с	до 1 Гбит/с	до 100 Мбит/с	до 100 Мбит/с
Дополнительно	-	-	-	2 порта Uplink, 1 Гбит/с
Габариты, мм	92 x 24 x 67	158 x 30 x 98	92 x 24 x 67	445 x 44 x 236
Подробности	www.asus.ru	www.asus.ru	www.linksysbycisco.com	www.cisco.com

На самом деле иногда связь по Wi-Fi по шифрованному каналу с направленными антеннами применяют для проброса радиомостов длиной в единицы километров по прямой видимости там, где прокладка кабеля не окупится. Я сталкивался с такой технологией в Крыму, например.

именно такие роутеры раздают «вафли» у нас в редакции и дома у хардреда. А владельцем ZyXEL NBG318S EE, если не ошибаюсь, является редактор софтового раздела.

Гидры многоглавые

Свичи, или, выражаясь официальным языком, сетевые коммутаторы, являются более простыми и «глупыми» устройствами, нежели роутеры. Они служат для связи компьютеров локальной сети между собой, а иногда – со шлюзом интернета. Раньше для этой цели применялись еще более примитивные средства – хабы (концентраторы). Хабы рассылали данные, пришедшие на один из портов, через все остальные порты. Свич ведет себя чуть умнее – он запоминает MAC-адреса сетевых карт, подключенных к его портам, и автоматически направляет фрейм, адресованный определенной сетевой карте из числа подключенных к нему, на соответствующий порт. Скорость работы таких девайсов, как правило, высока, однако дешевые (и за счет этого самые популярные, естественно) решения могут подтормаживать. Здесь мы приведем несколько достойных вариантов: рассмотрим парочку на пять портов, один на восемь и один совсем большой – для установки в стандартную 19-дюймовую стойку.

ASUS GigaX 1005

Первый из отобранных для обзора свичей относится к низшей ценовой категории и уже довольно ненов. Но, несмотря на это, он обеспечивает заявленную скорость локальной сети и не зависает, в отличие от некоторых конкурирующих моделей по той же цене. Дизайн коробочки не особо радует глаз, но функциональность ее на высоте.

ASUS GX-D1051

А заплатив всего в три раза больше, можно приобрести в десять раз более быстрое устройство (смайл). Этот свич с кавайной внешностью и, опять же, пятью портами поддерживает гигабитную сеть, чем в основном и интересен. Если для вас это необходимая опция, то GX-D1051 – ваш выбор.

Linksys SD208

Девайс с восьмью портами нужен далеко не в каждой локалке – часто хватает и меньшего количества. Но если вам требуется именно столько портов Ethernet, то можно смело порекомендовать Linksys SD208. Это, правда, не самый бюджетный вариант, зато он надежен. Из непрофессиональных решений, выпущенных фирмой Cisco, SD208 – едва ли не самый дешевый восьмипортовый коммутатор Ethernet. Несмотря на это, с работой в небольших сетях он справляется на «отлично».

Cisco Catalyst 2960-24TT

И наконец, последний аппарат в подборке присутствует скорее просто для того, чтобы вы оценили разницу в цене между свичами для малых локальных сетей и тяжеловесным сетевым оборудованием. Впрочем, возможности этого внушительного коммутатора тоже впечатляют весьма сильно. Он обладает огромной пропускной способностью (до 8,8 Гбит/с), имеет два гигабитных Uplink-порта и умеет работать с современными протоколами, обеспечивающими безопасность сети и интеллектуальное распределение ее пропускной способности. Ну и 24 порта Fast Ethernet – это немало.

Радиосвязь в пределах офиса

В обычных условиях устройства Wi-Fi используют именно для снабжения доступом к интернету пользователей на небольшой территории, чаще в помещении. Как вы могли заметить, роутеры, рассмотренные выше, имеют встроенные вайфайные точки доступа. Да и вообще, в непрофессиональном сегменте по-другому уже и не делают: попробуйте найти домашний маршрутизатор без Wi-Fi-модуля – я не уверен, что сможете. В связи с этим вопрос о точках доступа на некоторое время отложим, хотя, разумеется, не обойдем их вниманием. А пока разберемся с Wi-Fi-модулями для компьютеров.

При выборе беспроводной сетевой карты (Wi-Fi-модуля) следует смотреть на следующие характеристики: поддерживаемый стандарт Wi-Fi (сейчас актуальны g и n) и типы шифрования. Остальное не так важно, даже радиус действия: если его и указывают на коробке с устройством, то только для каких-то идеальных условий. Да, еще беспроводные сетевые карты бывают с разными интерфейсами. Самый универсальный (и последовательный (смайл)) из них, ясное дело, USB. Подключаемые к этому широко распространенному порту Wi-Fi-донглы и рассмотрим для начала.

TP-LINK TL-WN322G

Вот, например, вполне себе канонический Wi-Fi-адаптер с интерфейсом USB от фирмы TP-LINK, примечательный разве что очень низкой ценой. Небольшое устройство из разряда «воткнул и забыл» добавит поддержку беспроводных сетей компьютеру или ноутбуку, по умолчанию обделенному этой архиполезной функцией. Ждать от него сверхвысоких скоростей или особой дальности приема не стоит, но для мест, где Wi-Fi доступен хорошо, он подойдет в самый раз. А вот любители ловить халявные интернеты могут проходить дальше (смайл).

ZyXEL G-202 EE

Этот Wi-Fi-модуль отличается от собратьев прежде всего тем, что поставляется вместе с удлинителем-подставкой. Таким образом, использовать его удобней, чем большинство похожих на флэшки конкурирующих моделей. Этот донгл занимает только сам USB-порт, а не место вокруг него. Еще благодаря такой конструкции его можно переставлять с целью поимки наиболее стабильного сигнала, не сдвигая сам компьютер. Также хочется отметить стабильную работу девайса, в том числе с популярными сетевыми медиацентрами (см. далее). А еще он дружит с семейством ОС GNU / Linux.

К сожалению, у ZyXEL G-202 EE есть очень существенный недостаток: он не умеет работать в Windows 7 в качестве точки доступа, то есть из-под «семерки» с него нельзя раздавать беспроводный интернет. Но ловить-то можно! Поэтому многим устройство подойдет. Кстати, обратите внимание: оно рабо-

RSS

Направленную антенну для Wi-Fi- и, что нередко важнее, WiMAX-сетей можно сделать на основе цилиндрической коробки из-под популярных чипсов. Надо взять длинную упаковку в качестве отражателя волн. Конкретные «схемы сборки» есть в интернете.

Таблица 3. Технические **характеристики** Wi-Fi-донглов, сетевых карт и точек доступа

	TP-LINK TL-WN322G	ZyXEL G-202 EE	TRENDnet TEW-624UB	D-Link DWA-547	Linksys WMP300N	D-Link DWL-2100AP	Netgear WNAP210
Цена, руб.	420	1000	1500	1400	2800	2200	6000
Стандарт	Wi-Fi 802.11g	Wi-Fi 802.11g	Wi-Fi 802.11n	Wi-Fi 802.11n	Wi-Fi 802.11n	Wi-Fi 802.11g	Wi-Fi 802.11g
Шифрование	WEP, WPA, WPA2	WEP, WPA, WPA2, 802.1x	WEP, WPA, WPA2	WEP, WPA, WPA2	WEP	WEP, WPA, WPA2, 802.1x	WEP, WPA, WPA2, 802.1x
Интерфейс	USB 2.0	USB 2.0	USB 2.0	PCI	PCI	Ethernet	Ethernet
Габариты, мм	86 x 12 x 26	81 x 27 x 13	80 x 27 x 12 мм	134 x 121 x 19	134 x 121 x 19	109 x 31 x 142	109 x 31 x 142
Подробности	www.dlink.ru	www.zyxel.ru	www.trendnet.ru	www.dlink.ru	www.linksysby-cisco.com	www.dlink.ru	www.netgear.ru

тает с Wi-Fi 802.11g, а версию n не поддерживает.

TRENDnet TEW-624UB

Сей донгл беспроводной сети на первый взгляд выделяется лишь чуть более крупными размерами. А «пополнел» он на самом деле неспроста: в нем заложена поддержка самой быстрой на сегодня версии протокола Wi-Fi – 802.11n. Это означает, что он способен передавать данные на скорости до 300 Мбит/с против 54, характерных для прошлой ревизии. На практике, конечно, разница в скоростях меньше, но прирост относительно 802.11g все равно ощутим.

Однако не одним USB-интерфейсом живы Wi-Fi-адаптеры, и сейчас мы рассмотрим парочку решений для слота PCI. Да, десктопы тоже можно снабдить беспроводной связью, почему бы и нет? Иногда это удобно, например, если сделать сам комп точкой доступа.

D-Link DWA-547

Первая из двух приведенных нами Wi-Fi-карт для слота PCI более или менее обычна. Она имеет три штырьковые антенны, которые привинчиваются к ней стандартными разъемами и, соответственно, могут быть заменены. В остальном устройство ничем не примечательно, кроме способности держать связь по протоколу 802.11n, в том числе в режиме точки доступа, со всеми актуальными на сегодняшний день видами шифрования.

Linksys WMP300N

А вот вторая из отобранных для участия в параде сетевой техники десктопная Wi-Fi-карта выглядит менее тривиально. WMP300N комплектуется внешней антенной (точнее, тремя антеннами), которую благодаря тому, что она на проводе, можно установить выше самого системного блока. Это существенно увеличит зону покрытия беспроводной локальной сети. Собственно, большую часть цены данного сетевого адаптера составляет как раз цена антенны. И смысл приобретать такую штуку есть, если вы собираетесь раздавать Wi-Fi версии n с компьютера.

Таблица 4. Технические характеристики **антенн**

	D-Link ANT24-0801	ZyXEL Ext 109
Цена, руб.	3200	3000
Диапазон, ГГц	2,4	2,4
Усиление, дБи	8,5	9
Габариты, мм	120 x 120 x 43	114 x 114 x 40
Подробности	www.dlink.ru	www.zyxel.ru

Обратите внимание: устройство будет особенно полезным, если вы намереваетесь именно раздавать халявный Wi-Fi направо и налево, потому что единственный алгоритм шифрования, который этой радиосетевой карте доступен, весьма неустойчив ко взлому. Хотя можно рекомендовать девайс для подъема общественных Wi-Fi-сетей – на этом поприще его ждет несомненный успех.

Итак, адаптеры Wi-Fi мы рассмотрели. Теперь, чтобы закрыть тему беспроводных сетей, нужно глянуть на точки доступа, не интегрированные в роутеры. Разумеется, дорогие профессиональные решения нас мало интересуют, поэтому пройдемся по аппаратуре потребительского уровня.

D-Link DWL-2100AP

Например, вот точка доступа, сделанная уже известной вам фирмой D-Link. Она работает по стандарту Wi-Fi g, причем с определенными моделями беспроводных сетевых адаптеров той же фирмы умеет держать удвоенную скорость. К достоинствам устройства можно отнести приличную мощность сигнала, стабильность работы и поддержку современных видов шифрования. Да, антенны можно отвинчивать и заменять любыми другими. Кстати, эту точку доступа, вроде бы офисного назначения, удается использовать и для установления радиомоста, правда не со штатной антенной, конечно. И да, она может работать как ретранслятор Wi-Fi – что характерно, такая возможность есть не у всех девайсов, а она очень полезна.

Netgear WNAP210

Эта же точка доступа интересна тем, что совместима с 802.11n и, соответственно, должна гонять данные по эфиру существенно быстрее предыдущей героини статьи. Она не имеет внешних антенн. Эстетически это правильно – здоровый минимализм, кто бы спорил. Однако вопрос о том, как их отсутствие отражается на качестве покрытия, остается открытым. Вроде бы устройство работает вполне прилично. Но сказать честно, за шесть тысяч хочется больше возможностей. Ну, хотя бы вход для отдельной антенны не помешал бы. Устройство комплектуется пожизненной гарантией.

дБи – изотропный децибел (децибел относительно изотропного излучателя). Характеризует коэффициент направленного действия (а также коэффициент усиления) антенны относительно коэффициента направленного действия изотропного излучателя. (Wiki)

Рассмотрев точки доступа, можно, казалось бы, переходить от оборудования для беспроводных сетей к другим устройствам. Однако самое время вспомнить про антенны, которые приобретаются отдельно. Рассмотрим хотя бы две штуки.

D-Link ANT24-0801

Первая имеет стандартный вид и может быть подвешена на стенке в офисе без риска испортить интерьер. Ее дизайн сделан так, чтобы вписываться в обстановку любой конторы. А технические характеристики вы найдете на стр. 27.

ZyXEL Ext 109

Вторая антенна ориентирована на работу на улице, а не в помещении. Недаром в ее названии фигурирует буквосочетание «Ext», что значит «external», то есть «наружная». Выглядит она, кстати, очень стильно и поставляется в комплекте с кронштейном. Производитель утверждает, что она приспособлена для всепогодных условий и годится для организации радиосвязи на расстоянии до 5 км. Это похоже на правду.

И вот на этой жизнерадостной ноте с беспроводными сетями можно наконец покончить. Хотя это утверждение касается только Wi-Fi-сетей, ведь есть и другие протоколы беспроводной связи, ну да о них не в этот раз.

Сохранить и всем раздать

С этими взаимоисключающими на первый взгляд задачами успешно справляются системы сетевого хранения данных (Network Attached Storage, NAS). Они состоят из накопителя (одного или нескольких жестких дисков) и коробки, внутри которой находится небольшой, холодный, маломощный и, как правило, одноплатный специализированный компьютер. Он в состоянии работать файловым сервером по нескольким протоколам («виндовому» SMB, «линуксовому» NFS, а также FTP) и иногда имеет дополнительные возможности вроде торрент- или FTP-клиента. Его операционная система – прошивка устройства – чаще всего основана на Linux, так что количество дополнительных функций зависит в основном от размаха фантазии разработчика девайсины, а их работоспособность – еще и от мощности аппаратной начинки.

NAS обязательно имеет отсек для дисков и интерфейс проводной сети. Этот набор может быть дополнен разъемами под внешние носители, беспроводным адаптером и другими полезными мелочами. От просто коробки для жестких дисков NAS отличается наличием LAN-порта.

Собственно, в былые времена в качестве таких вот файлохранилищ часто использовались маломощные компьютеры. А теперь выпускают специальные устройства, недорогие и хорошо заточенные под свою основную задачу. Как минимум таковы некоторые из них (смайл). Ну, начнем, пожалуй.

Western Digital WDG2NC10000

И начнем мы с недорогого и компактного варианта. Это устройство эволюционировало до сетевого файлохранилища из обычного внешнего диска. Ну, хорошо, пусть не из обычного, а из очень стильного, и красивого, и качественного, и достаточно быстрого... стоп, а это уже совсем другое дело. Итак, данный представитель благородного семейства западных цифровых дисков Western Digital My Book отличается от родственных моделей как раз наличием порта Ethernet, причем гигабитного. Возможностей у него, по совести сказать, не фонтан как много. Ни тебе FTP-сервера (или тем более клиента), ни медиасервера... но хранить данные на нем можно, и доступ к ним будет быстрый. Работает девайс, кстати, негромко, а выглядит сами видите, как здорово. Ни в офисе, ни дома он не помешает.

Acer Aspire easyStore H340

Теперь посмотрим на более каноническую модель, произошедшую скорее от полноценных файловых серверов путем урезания их мощности и сокращения габаритов. Вообще, данный девайс сложно назвать типичным не только из-за железных, но и из-за софтовых характеристик. Так, в качестве ОС тут вовсе не вариация на тему GNU / Linux, а ровно наоборот – Windows Home Server. Однако конфигурация и набор возможностей девайсины впечатляют. Она содержит четыре дисковых отсека, причем в трех из них диски можно заменять «на горячую», как в полновесном сервере. А вот RAID-массивы данная модель, в отличие от, как ни странно, предыдущей, не поддерживает. Это не особо радует. Но зато в комплекте идут два жестких диска по 750 Гбайт, а в принципе можно установить их четыре штуки, каждый объемом 1,5 Тбайт. Впечатляет, не правда ли?

По очевидным причинам девайсина отлично впишется в сеть, состоящую из компьютеров под Windows. Впрочем, если вам нужны какие-то возможности, которые в Windows Home Server реализованы криво или отсутствуют, можно попробовать поставить другую ОС. Открыв корпус, можно инсталлировать на матплату устройства подходящую для разъема PCIE x4 видеокарту (скажем, с интерфейсом PCIE x1). А после этого уже вполне удастся переустановить «ось».

В общем, NAS вышел у Acer однозначно интересный, но не для всех – это факт. Да и цена устройства отнюдь не демократичная, кстати.

QNAP TS-459 Pro+

А вот теперь наконец-то глянем на самого что ни на есть характерного представителя класса. TS-459 Pro+ работает под управлением Embedded Linux и имеет четыре посадочных места под винчестеры. Он умеет объединять их в RAID-массивы уровней 0, 1, 5, 6 и JBOD. Еще NAS поддерживает стандартные для свободной ОС файловые системы EXT3 и EXT4, а также NTFS и FAT-32 (для внешних дисков). Взаимодействовать с другими машинами локальной сети данный девайс может по протоколам SMB, FTP, NFS, HTTP / HTTPS, SSH, iSCSI и еще нескольким более экзотическим. Такая функцио-

RSS

Wi-Fi Protected Setup (WPS) – стандарт автоматического создания беспроводной домашней сети. В простейшем случае вся настройка сводится лишь к нажатию кнопок настройки на точке доступа и подключенных устройствах.

нальность характерна далеко не для всех сетевых коробок с файлами.

Быстродействие устройства вас, скорее всего, порадует, но объединять винты в RAID 0 ради его повышения нет смысла. Лучше сделать «зеркало» или поднять массив RAID 5 для надежности хранения ценных данных. И последнее: приобретая девайс, не забудьте, что винтов в комплекте нет. Их нужно будет купить отдельно. Впрочем, учитывая стоимость самого устройства, это будет не очень существенная трата (смайл).

Играющие с носителями

За этим хитрым словосочетанием я решил скрыть такой класс устройств, как медиаплееры. На самом деле играют они скорее «с носителей». Сетевые проигрыватели отличаются от любых других тем, что у них носитель контента находится не в самом аппарате, а удален от него. Связь между проигрывателем и накопителем осуществляется через ЛВС. Классический медиаплеер – маленький, почти незаметный рядом с телевизором аппаратик более или менее прямоугольной формы, с гнездом Ethernet и цифровыми выходами для изображения и звука (чаще всего HDMI). Остальные характеристики могут меняться от модели к модели. Эти симпатичные девайсы позволяют с удобством смотреть фильмы и слушать музыку из домашней локальной сети.

WD TV Live

Первая модель, которую мы рассмотрим, называется WD TV Live – коротко и ясно. Кроме разъема проводной сети девайсина имеет также два USB-гнезда. К ним можно подключать носители данных – флэшки, жесткие диски, – а можно Wi-Fi-модули, однако не любые. Рассмотренная выше по тексту модель фирмы ZyXEL как раз одна из немногих подходящих, но не единственная. На сайте производителя есть полный их список.



Сетевые проигрыватели отличаются от любых других тем, что у них носитель контента находится не в самом аппарате, а удален от него. Связь между проигрывателем и накопителем осуществляется через ЛВС.

Тем временем я рекомендую связать плеер с локальной сетью все же кабелем, потому что гнать широкий поток видео высокой четкости лучше, на мой вкус, по твердой, надежной меди, а не по зыбким волнам эфира (смайл). Впрочем, это лирика, а на практике чаще всего и «толщины» Wi-Fi-канала хватает (во всяком случае, версии g).

Плеер действительно умеет читать почти любые форматы видео, как высокой, так и средней четкости. У него есть полезная (хотя за счет отсутствия клавиатуры не очень удобная) функция просмотра роликов с YouTube. Управляется эта штука исключительно с пульта – не теряйте его ни в коем случае! Кстати, с проигрыванием звука все тоже достаточно интересно: кроме выхода HDMI, по которому звук идет вместе с изображением, имеется оптический S/P-DIF. Владельцы многоканальных систем ликуют (смайл). Ну, и последнее: быстродействие девайса на высоте – торможения не замечено ни при показе кино, ни при навигации по меню.

Iconbit HDS41L

Сетевой мультимедийный плеер HDS41L представляет собой весьма продвинутую и стильно выглядящую конструкцию. Винчестера в комплекте нет, диски стандарта SATA 2,5" вставляются сбоку. Поддерживаются форматы видео HD / SD, MPEG-1 / -2 / -4, DivX, HDV, HDTV, AVCHD (H.264), MKV – ну то есть практически все, которые на данный момент могут считаться актуальными. Помимо этого аппарат воспроизводит музыку, пожатую кодеками MP3 / WMA / FLAC, и, разумеется, понимает изображения в формате JPEG. Для пущего удовольствия на борту Iconbit HDS41L вы найдете порты eSATA, HDMI 1.3, компонентный и композитный выходы, ну и, естественно, разъем для подключения кабеля локалки. Плеер может быть рекомендован всем желающим создать у тебя в домашней сети хранилище видео- и аудиоданных и при этом не напрягать себя сложными настройками и борьбой с конфликтами устройств.

Малой сети – много устройств

Итак, вот и подошел к концу наш обзор домашнего сетевого оборудования. Мы постарались выбрать лучшие или по крайней мере примечательные устройства. Просмотрев их описания и характеристики, вы сможете определиться с девайсами для собственной сети, зная, на какие ТТХ надо обращать внимание, а за что можно и не переплачивать. Желаем вам маленьких пингов и уверенного приема (смайл)! UP

Таблица 5. Технические характеристики сетевых хранилищ (NAS)

	Western Digital WDG2NC10000	Acer Aspire easyStore H340	QNAP TS-459 Pro+
Цена, руб.	4800	16 000	36000
Количество отсеков для HDD	2	4	4
Поддержка RAID	RAID 1	отсутствует	RAID 0, 1, 5, 6, JBOD
HDD в комплекте	2 x 500 Гбайт	2 x 500 Гбайт	нет
Габариты, мм	104 x 175 x 160	300 x 305 x 330	180 x 235 x 185
Подробности	www.wdc.com/ru	www.acer.ru	www.qnap.com

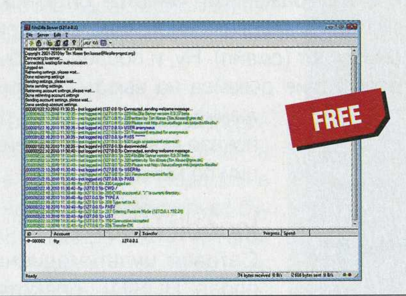
Таблица 6. Технические характеристики сетевых медиаплееров

	WD TV Live	Iconbit HDS41L
Цена, руб.	3600	3500
Видеовыход	HDMI 1.3	HDMI 1.3
Интерфейсы	2 x USB 2.0	2 x USB 2.0, eSATA
Отсек под HDD	нет	есть
Дополнительно	S/P-DIF out	S/P-DIF out
Габариты, мм	125 x 40 x 100	155 x 40 x 115
Подробности	www.wdc.com/ru	www.iconbit.ru

Стандарт беспроводных сетей IEEE 802.11n появился 11 сентября 2009 года. Устройства данного стандарта могут работать в одном из двух частотных диапазонов – 2,4 или 5 ГГц. Это намного повышает гибкость их применения, позволяя отстраиваться от источников радиопомех. (Wiki)

FTP-сервер FileZilla Server 0.9.37

Если вам нужен мощный и быстрый FTP-сервер для Windows, то он перед вами. Поддерживаются протоколы FTP / SFTP / FTPS, в наличии система управления пользователями, группами и правами доступа. FileZilla Server обрабатывает файлы, в именах которых присутствуют кириллические символы. При этом его компоненты занимают в памяти меньше 3 Мбайт.



- **Разработчик:** Tim Kosse
- **ОС:** Windows XP / Vista / 7 (32 и 64 бит)
- **Объем дистрибутива:** 1,6 Мбайт
- **Русификация интерфейса:** нет
- **Адрес:** filezilla-project.org

Утилита TimeSync 2.0

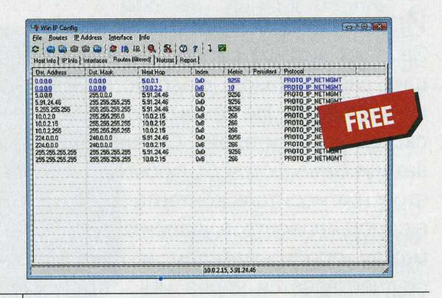
Несмотря на то что эта утилита для синхронизации времени не обновляется уже несколько лет, она работает во всех версиях Windows. Дозволяется не только вручную указывать серверы NTP, но и выбирать, с какой периодичностью нужно к ним обращаться. Все настройки хранятся в файле INI, и установки в систему TimeSync не требует. А вот встроенной справки нет.



- **Разработчик:** Ravi Bhavnani
- **ОС:** Windows 98 / Me / 2000 / XP / Vista / 7 (32 и 64 бит)
- **Объем дистрибутива:** 612 Кбайт
- **Адрес:** www.ravib.com/timesync

Конфигуратор Win IP Config 2.7.2

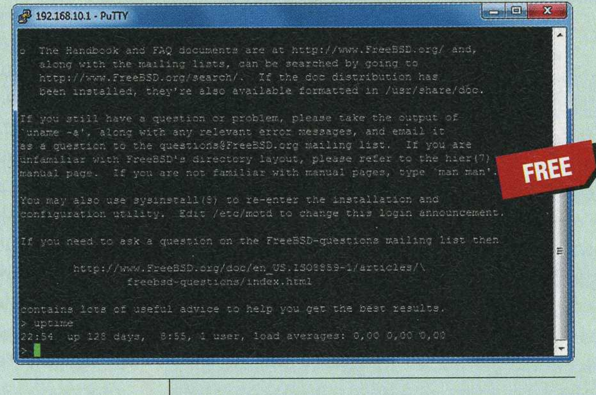
Тем, кто не желает пользоваться штатными консольными утилитами «Винды» для изменения таблиц сетевых маршрутов, можно предложить данную утилиту. Это графическая оболочка для команд `ipconfig`, `route` и `netstat`, которая позволяет просматривать / удалять / добавлять маршруты, включать и выключать сетевые интерфейсы и знакомиться со статистикой по адаптерам.



- **Разработчик:** Peter Kostov
- **ОС:** Windows XP / Vista / 7 (32 и 64 бит)
- **Объем дистрибутива:** 1 Мбайт
- **Русификация интерфейса:** нет
- **Адрес:** www.pkostov.com/wipcfg.html

Терминальный клиент PuTTY 0.60

Те, кому по долгу службы приходится админить удаленный Unix-сервер с «виндовой» машины, свой выбор сделали давно: PuTTY – вероятно, самый удобный терминальный клиент. Объясняется это не только его бесплатностью, но и поддержкой всех протоколов (SCP, Telnet, SSH обеих версий и SFTP), а также эмуляцией терминалов. Правда, для передачи файлов придется использовать консольный клиент, но разве настоящего линуксоида это остановит (смайл)? Кстати, возможно соединение с удаленным хостом через прокси-серверы.

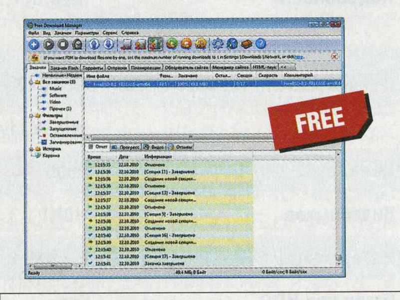


- **Разработчик:** Simon Tatham
- **ОС:** Windows XP / Vista / 7 (32 и 64 бит)
- **Объем дистрибутива:** 1,44 Мбайт
- **Русификация интерфейса:** нет
- **Адрес:** www.chiark.greenend.org.uk/~sgtatham/putty

Программа корректно отображает кириллические символы – если, конечно, на «юниксовой» машине сделаны соответствующие настройки. Отрадно, что рамки популярного файлового менеджера Midnight Commander тоже отрисовываются корректно. Есть и функция сохранения в профилях настроек подключения, так что пользователь избавлен от необходимости запоминать кучу адресов и паролей.

Менеджер загрузок Free Download Manager 3.0

FDM – это настоящий «комбайн»: здесь есть не только качалка файлов, поддерживающая протоколы HTTP / HTTPS / FTP, но также клиент BitTorrent, офлайновый браузер и мощный планировщик заданий. Разумеется, многопоточная загрузка и докачка поддерживаются в лучшем виде. Прога умеет следить за буфером обмена, а также интегрируется со всеми распространенными обозревателями Сети.



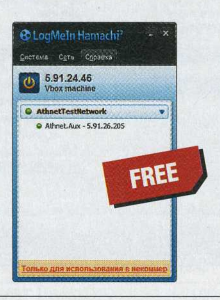
- **Разработчик:** Free Download Manager.ORG
- **ОС:** Windows XP / Vista / 7
- **Объем дистрибутива:** 6,71 Мбайт
- **Русификация интерфейса:** есть (полная)
- **Адрес:** www.freedownloadmanager.org

RSS

Мы собрали в этой рубрике те сетевые программы для Windows, которыми пользуемся сами. Так что можно сказать, что на следующих четырех страницах вы найдете квинтэссенцию нашего многолетнего опыта тестирования ПО.

Менеджер VPN Hamachi 2.0.2.85

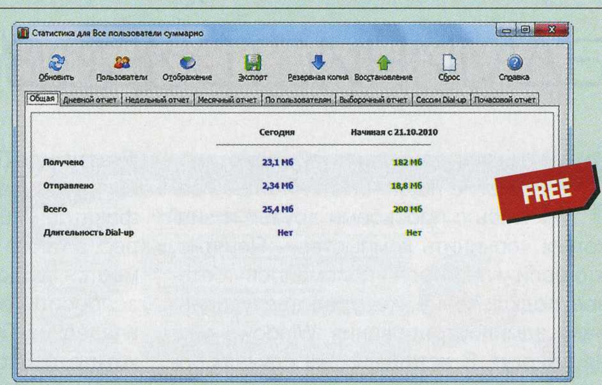
Желаете организовать собственную приватную сеть? В бесплатном для некоммерческого использования варианте возможно объединение в сетях VPN до 16 узлов – этого более чем достаточно для домашних пользователей. При этом все данные, передаваемые по открытым каналам, шифруются по алгоритму AES-256. В защищенной сети можно, например, играть в игры.



- **Разработчик:** LogMeIn
- **ОС:** Windows XP / Vista / 7 (32 и 64 бит)
- **Объем дистрибутива:** 3,14 Мбайт
- **Адрес:** www.logmein.com/products/hamachi2

Монитор трафика NetWorx 5.1.4

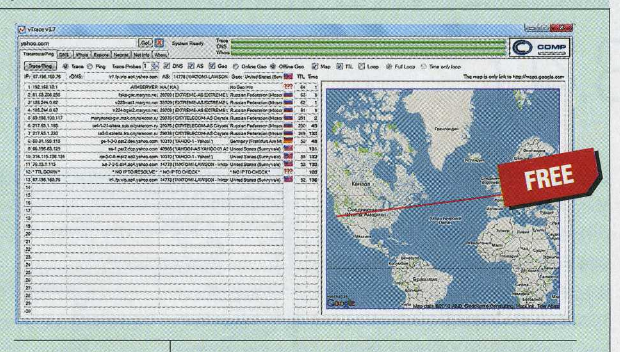
Вероятно, на просторах нашей необъятной родины еще немало осталось тех, кто вынужден считать каждый скачанный из Сети мегабайт. Порекомендуем им NetWorx, потому что в этой программе есть все, что нужно, и ничего лишнего. Она может мониторить любой сетевой интерфейс, показывать статистику по часам / дням / неделям / месяцам, а также по каждому из пользователей системы. Для тех, кто сидит на диалапе, имеется отдельный раздел в отчете, где собрана информация по всем сеансам связи. Дозваниваться до провайдера софтина тоже умеет. При превышении лимита NetWorx может сообщить об этом юзеру, автоматически разорвать соединение, запустить выбранное приложение либо же выключить ПК. Есть функция экспорта статистических данных в файлы форматов XLS / DOC / HTML / TXT / CSV. Доступ к настройкам защищается паролем.



- **Разработчик:** SoftPerfect Research
- **ОС:** Windows XP / Vista / 7 (32 и 64 бит)
- **Объем дистрибутива:** 1,5 Мбайт
- **Русификация интерфейса:** есть (полная)
- **Адрес:** www.softperfect.com/products/networx

Набор сетевых утилит vTrace 3.7.7.4

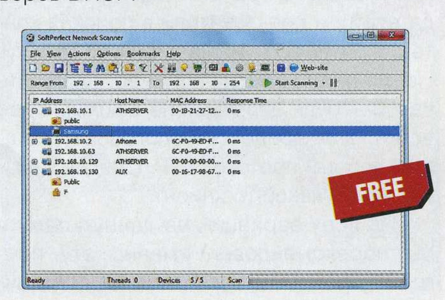
Разработчики из Редмонда обделили Windows сетевыми утилитами, но польский автор исправил это недоразумение, написав бесплатную программу типа «все-в-одном». В ней вы найдете команды `traceroute`, `ping`, `whois`, `dig` (здесь она называется DNS) и netstat, а также простенький сетевой сканер. Разобраться с vTrace не составит труда: надо лишь указать имя или адрес хоста да нажать кнопку Go!. Радует, что к софтине можно «прикрутить» базу MaxMind GeoIP, после чего при выполнении команды `traceroute` будет автоматически определяться географическое местоположение всех узлов. Кстати, при желании vTrace отобразит найденный маршрут на карте мира (для этого используются средства Google Maps). Разумеется, для команд `whois` и `nslookup` можно указать серверы, которые нужно опрашивать. Имеется портативная версия приложения. К сожалению, официальный сайт на момент написания этой заметки был в офлайне. Ссылку на загрузку дистрибутива вы легко найдете на портале Softpedia.com.



- **Разработчик:** Arkadiusz Nowicki
- **ОС:** Windows XP / Vista / 7 (32 и 64 бит)
- **Объем дистрибутива:** 975 Кбайт
- **Русификация интерфейса:** нет
- **Адрес:** www.vtrace.pl

Сканер сетей SoftPerfect Network Scanner 5.0.3

Программа способна просканировать диапазон адресов и найти на обнаруженных узлах открытые порты. Для хостов, использующих протокол NetBIOS, автоматически определяются «расшаренные» ресурсы. Есть возможность получения информации с устройств, поддерживающих протокол SNMP. Кроме того, вы найдете здесь множество встроенных утилит, к примеру для поиска в сети серверов DHCP.

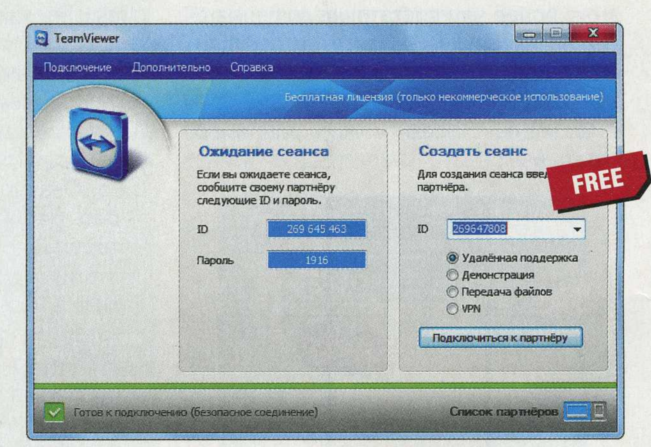


- **Разработчик:** SoftPerfect Research
- **ОС:** Windows XP / Vista / 7 (32 и 64 бит)
- **Объем дистрибутива:** 720 Кбайт
- **Адрес:** www.softperfect.com/products/networkscanner

Ну а коль скоро весь предложенный нами софт абсолютно бесплатен (это мы специально так сделали! – Прим. ред.), вы сможете установить его сразу после того, как поселите в своем новом компьютере операционную систему и обеспечите ей выход в интернет.

Средство удаленного администрирования TeamViewer

Начну с банальностей: вероятно, многие наши читатели сталкивались с просьбами друзей и знакомых «починить компьютер». Понятно, что если у приятеля «поломалось» сетевое подключение, то средства удаленного администрирования Windows уже не помогут. В остальных же случаях подобного рода ПО способно сильно облегчить жизнь добровольному помощнику, ибо ему не придется ехать в гости к незадачливому юзеру. TeamViewer, конечно, не единственная программа, позволяющая управлять удаленной машиной, но одна из самых удобных. По умолчанию творение немецких разработчиков использует для связи с сервером исходящие соединения на TCP-порт 80, что избавляет от необходимости настраивать файрволл (в настройках дозволяется выбирать и прямое соединение по IP-адресу). Для подключения надо ввести идентификатор машины либо адрес, а также пароль (разумеется, вы должны сначала запросить эти данные у владельца ПК, к которому хотите подсоединиться) и указать режим работы. Всего их четыре: «Удаленная поддержка» (администрирование чужой машины), «Демонстрация» (показ своего «Рабочего стола» без возможности управления компьютером), «Передача файлов» и VPN (создание частной защищенной сети). В первом из этих режимов вы можете делать на удаленном компьютере то же, что и ваш партнер (например, запускать приложения). UP



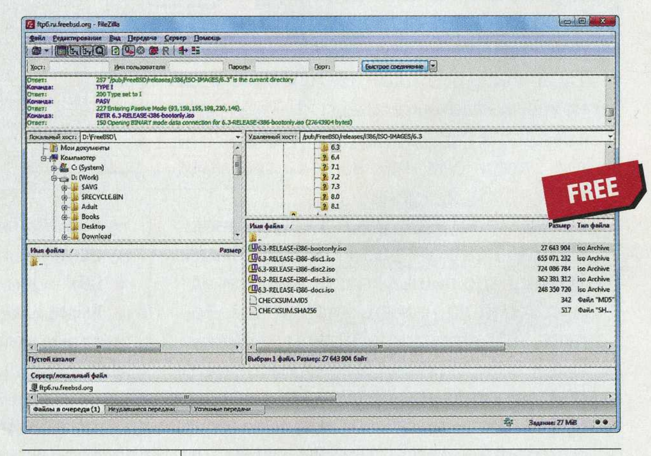
- **Разработчик:** TeamViewer GmbH
- **ОС:** Windows 95 и выше (32 и 64 бит)
- **Объем дистрибутива:** 2,98 Мбайт
- **Русификация интерфейса:** есть (полная)
- **Адрес:** www.teamviewer.com/ru/index.aspx

FTP-клиент FileZilla 3.3.4.1

Лет пять-десять назад в каждой уважающей себя домашней сети был собственный FTP-сервер (и, как правило, не один). Сегодня такой способ обмена файлами уже неактуален («благодарить» за это надо правообладателей), и пользователи в поисках контента переместились в пиринговые сети. Но если вы хотите, например, загрузить какой-нибудь дистрибутив Linux, скорее всего, вам придется использовать старый добрый протокол FTP. Следовательно, нужен какой-то клиент.

Из всех вариаций на данную тему я бы порекомендовал именно эту программу родом из Германии. Ее достоинства – поддержка практически всех расширений протокола FTP, защита соединения при помощи SFTP / FTPS / FTPES, умение работать с прокси-серверами, а также наличие встроенного менеджера хостов. Докачка файлов, разумеется, тоже возможна. Помимо прочего этот кросс-платформенный и оупенсорсный клиент отличается весьма скромными системными требованиями. Интерфейс удобный и понятный, прямо-таки классический, так что разобраться с софтиной под силу любому.

Недостаток один: нет планировщика заданий, причем автор, похоже, и не собирается реализовывать данную функцию, хотя пользователи на протяжении нескольких лет просят его об этом. В остальном же придраться совершенно не к чему. Кстати, FileZilla стабильно входит в десятку самых популярных приложений на сайте SourceForge.net. UP



- **Разработчик:** Tim Kosse
- **ОС:** Windows XP и выше, Linux, FreeBSD, Mac OS X
- **Объем дистрибутива:** 4 Мбайт
- **Русификация интерфейса:** есть (полная)
- **Адрес:** filezilla-project.org

RSS

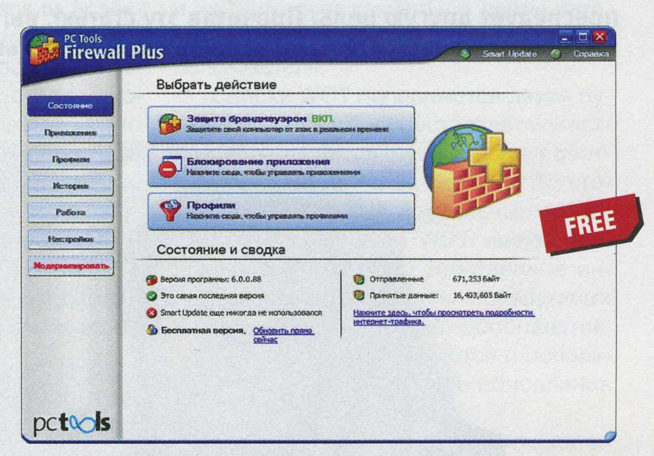
Автором рубрики «UPgrade рекомендует» является Михаил Задорожный, с которым всегда можно связаться по e-mail: zmike@upweek.ru. Приветствуются любые предложения, пожелания по возможности тоже будут учтены.

Брандмауэр PC Tools Firewall Plus 6

Более-менее нормальный файрволл в ОС от Microsoft мы так и не увидели. Тот, что был в старушке XP, язык не поворачивается назвать межсетевым экраном – настолько он примитивен. А тот, который появился в «Висте» и «семерке», был бы вполне хорош, если бы не кошмарный интерфейс.

Из всех отсмотренных мною брандмауэров я остановил свой выбор именно на этом. Во время установки будьте бдительны: вам попытаются, что называется, «впарить» панель инструментов Google для браузера и «шароварный» PC Tools Spyware Doctor. По завершении инсталляции последует неизбежная в таких случаях перезагрузка ПК.

Есть два режима работы – «Обыкновенный пользователь» (по умолчанию) и «Опытный пользователь». Я бы рекомендовал задействовать второй – тогда вы сможете создавать собственные правила как для приложений, так и для протоколов (в условиях дозволяется использовать адреса, подсети, номера портов, направление трафика и другие параметры). Делается все это с помощью весьма удобного мастера, так что проблем возникнуть не должно. Еще одна особенность PC Tools Firewall Plus – поддержка профилей, в которых можно задать собственный набор правил. Ну и, наконец, отмечу, что этот файрволл довольно бережно относится к системным ресурсам: все компоненты оного занимают в памяти меньше 15 Мбайт. UP



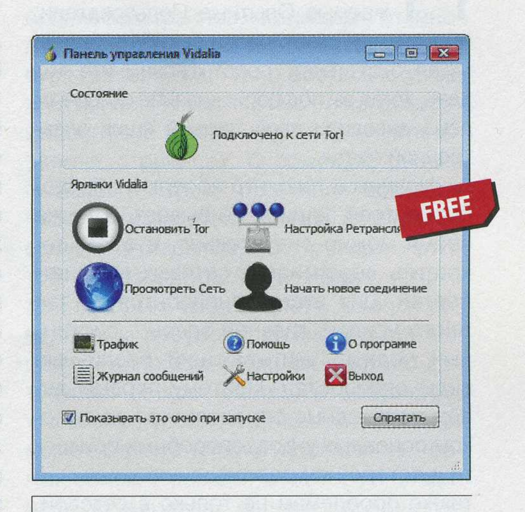
- **Разработчик:** PC Tools
- **ОС:** Windows XP и выше (32 и 64 бит)
- **Объем дистрибутива:** 10,21 Мбайт
- **Русификация интерфейса:** есть (полная)
- **Адрес:** www.pctools.com/ru/firewall/

Средство анонимизации Tor 1.3.10

Мы, конечно, живем не в Китае, где какой-нибудь диссидент, написавший в своем блоге про события на площади Тяньаньмэнь, легко может угодить за решетку. Но полагаю, что и для многих российских пользователей проблема обеспечения анонимности в Сети тоже актуальна. Дяденьки из Пентагона в свое время придумали распределенную сеть Tor, с помощью которой можно скрыть свой реальный IP-адрес, а потом взяли да и рассекретили проект. Сейчас его развивает американская некоммерческая организация, а исходный код находится в свободном доступе, что позволяет всем заинтересованным людям его совершенствовать.

При соединении с удаленным сервером сетевые пакеты от клиентской машины, на которой установлен Tor, проходят через цепочку хостов, расположенных в самых разных частях света. Эти узлы последовательно подменяют IP-адрес в заголовках пакетов, так что выследить отправителя практически невозможно. Тут важно понять следующее: Tor скрывает только реальный айпишник, но не данные, которые, например, браузер сообщает HTTP-серверу. Но хватит теории.

Для установки проги надо скачать дистрибутив Vidalia Bundle для своей платформы, а затем подсоединиться к сети Tor. Теперь о применении: браузерам надо приказать использовать прокси-сервер, который запущен на локальной машине (адрес 127.0.0.1) и «висит» по умолчанию на порту 8118. Для других сетевых приложений (например, месседжеров) есть SOCKS-прокси (порт 9050). Только учтите: программы, которые не умеют работать через прокси, подружить с Tor невозможно в принципе. UP



- **Разработчик:** The Tor Project
- **ОС:** Windows XP и выше (32 и 64 бит), Linux, FreeBSD, Mac OS X, Android, Apple iOS
- **Объем дистрибутива:** 2,29-10,60 Мбайт
- **Адрес:** www.torproject.org

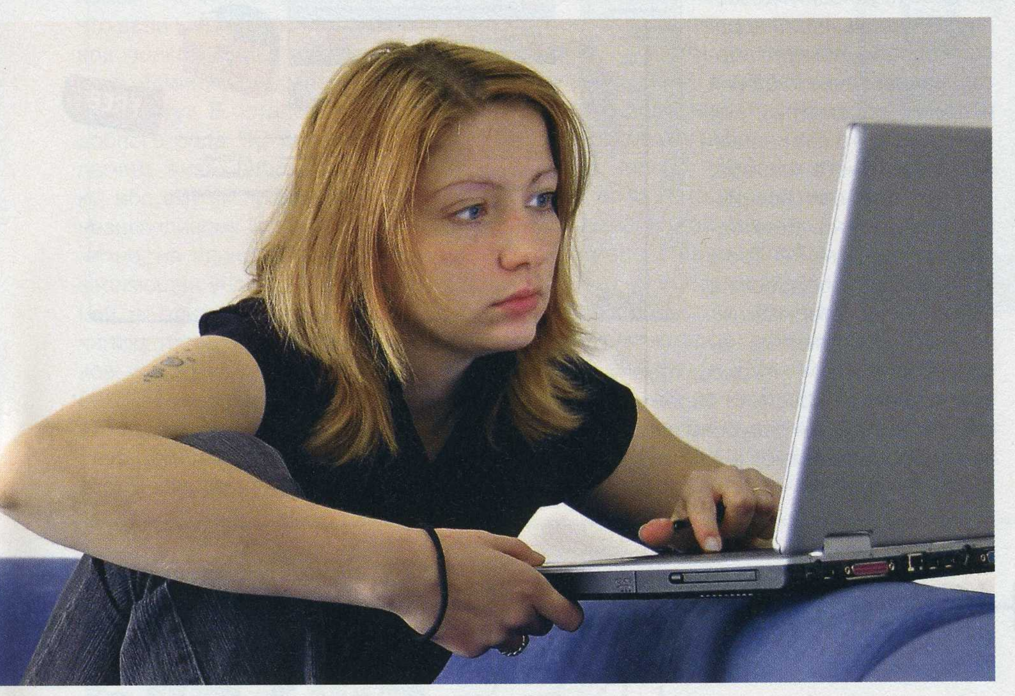
Если вы знаете какую-нибудь полезную и бесплатную программку, о которой мы еще не рассказали, присылайте ссылку на нее на адреса: zmike@upweek.ru или b@upweek.ru. В случае если софтина окажется интересной, она обязательно появится в рубрике «Маленькие программы».

О безопасном серфинге

На тему безопасности работы с ПК исписаны тома, поэтому пытаться охватить весь спектр сетевых «страшилок» было бы наивно. Наш рассказ преследует другую цель. Прочитав эту статью, вы сможете действительно серьезно повысить безопасность своей работы.



Алексей Кутовенко
soft@upweek.ru
Mood: рабочее
Music: Triumvirat



Наш обзор предназначен для начинающих юзеров. Поэтому, уважаемые Опытные Пользователи, прежде чем скептически выгибать бровь, читая этот текст, просто вспомните тот день, когда вы под попискивание dialup-модема заводили свой первый ящик электронной почты.

Начнем с того, что абсолютной, стопроцентной защиты не бывает. В то же время можно значительно, в разы сократить вероятность сетевых неприятностей. Для этого понадобится не так много усилий, главное здесь – системный подход, учитывающий различные виды опасностей. Поэтому первым делом необходимо определиться со списком основных угроз, способных привести к потере или разглашению данных, а также проблемам не только в сетевой, но и в реальной жизни. Почетное первое место в этом списке займут не вирусы и не хакеры, а сам пользователь, который по невнимательности или незнанию, образно выражаясь, иногда сам копает себе яму, да еще и укладывает на ее дно грабельки.

Аутотренинг

Если почитать книжки самого, наверное, «раскрученного» хакера современности Кевина Митника, то обнаружится любопытная вещь: большинство успешных взломов были осуществлены с помощью так называемого «социального инжиниринга», или, говоря проще, банального обмана пользователя. С той поры прошло немало времени, технологии шагнули вперед, а вот методы проникновения в систему «с помощью» самого юзера остаются одним из главных средств в арсенале всяческих мутных людей. Чтобы не оказаться в положении человека, который сам становится главной проблемой для собственной безопасности, достаточно соблюдать ряд несложных правил сетевой гигиены. Они банальны, но не потому, что скучны, а потому, что проверены тысячами ситуаций.

Самый простой и надежный способ избежать утечки особо чувствительных данных – по возможности не оставлять в Сети критичные персональные сведения. Размещая на онлайновом ресурсе какую-либо информацию о себе, сделайте паузу и представьте, что она подписана не ником, а вашим настоящим именем и вы рассказываете ее вашему потенциальному недоброжелателю. Если вы испытываете сомнения, лучше просто не выкладывайте ее. И на солнце бывают пятна, и даже самый серьезный поставщик интернет-сервисов не застрахован от сбоев. Стопроцентные гарантии может дать только бог или шарлатан. Более того, при наличии желания, времени и мотивации персональная информация (реальное имя, адрес, телефон и другие контактные данные) может быть извлечена даже из незначительных исходных данных, оставленных в сетевых источниках. Не будем пересказывать методы и примеры такой деятельности – отправьте на любом крупном поисковике запрос «деанонимизация», почитайте поучительные истории других людей и никогда не совершайте таких ошибок.

Незакрытый на чужом или общем компьютере почтовый аккаунт, пароль, записанный на бумажке, оставленной рядом с монитором, – список подобных ошибок можно продолжать. Соблюдайте элементарную осторожность в реале и не вводите ближних своих в искушение. Ибо при взломе аккаунта каких-нибудь «Одноклассников», скорее всего, стоит сетовать не на мифического хакера, а на собственную неосторожность. Кстати, о паролях: желательно не использовать одинаковые «волшебные слова» на различных сервисах. Если вам сложно придумывать пароли, воспользуйтесь простейшим мнемотехническим приемом: вспомните любимый стишок и составьте пароль, например, из первых букв его строчек. Пароли, как и носки, периодически следует менять.

RSS

Фишинг (англ. phishing, от fishing – рыбная ловля, выуживание) – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям. (Wiki)

Отказ от перехода по ссылкам, полученным из неизвестного источника по почте или ICQ, или же скачивание присланных таким способом файлов у осмотрительного интернетчика должен быть развит на уровне рефлекса и быть включенным по умолчанию. Помните, что некоторые «троянские кони» даже умеют поддерживать несложную беседу в чате для того, чтобы убедить пользователя щелкнуть по ссылке. Точно так же относитесь и к «официальным» просьбам выслать пароль, например, от почтового ящика – ни один нормальный «техсаппорт» никогда такого не попросит.

Всевозможные навороты современного сетевого софта, связанные с безопасностью, были придуманы вовсе не для того, чтобы позлить пользователей, а для того, чтобы уберечь их от типичных ошибок. Да, такие системы могут быть надоедливы, однако, если вам советует немедленно их отключить, например, зашедший в гости приятель, подумайте. Такие действия нужно выполнять только хорошо понимая их последствия, в идеале – одновременно с подключением каких-либо альтернативных средств защиты. Если уж вы обращаетесь за помощью, обязательно просите объяснить смысл производимых операций. И пусть это объяснение будет доступным. Если вы, именно вы, не понимаете смысл предлагаемых действий, лучше оставьте все как есть, мягко отстраните приглашенного эксперта от клавиатуры и займите его руки чашкой чая и вкусным бутербродом.

С точки зрения дополнения WOT сайт UPgrade вполне безопасен

Готовим доспехи

Теперь перейдем к техническим аспектам: попробуем классифицировать угрозы, возникающие в ходе серфинга, и поискать на них адекватные ответы. Современные сетевые программы – это сложные системы, в которых могут быть недоработки или бреши безопасности. Не забывайте поддерживать их в актуальном состоянии, вовремя устанавливайте обновления.

Про необходимость наличия антивирусного софта, а еще лучше комплексного решения, содержащего межсетевой экран (он же файрволл, или брандмауэр), долго говорить не стоит – это обязательное условие безопасности, реально способное защитить вас и окружающих от многих проблем.

Незакрытый на чужом или общем компьютере почтовый аккаунт, пароль, записанный на бумажке, оставленной рядом с монитором, – список подобных ошибок можно продолжать.

Основной инструмент интернет-работы – это браузер. Защитить его можно различными способами, в том числе и установкой различных дополнений. О них мы и поговорим далее.

Вряд ли здравомыслящий и находящийся в трезвом уме человек выберет для вечерней прогулки темные подворотни неблагополучного городского района. Аналогичный принцип следует использовать и в ходе серфинга. Многие сайты вольно или невольно становятся разносчиками всевозможной киберзаразы. Не будем забывать и об угрозе фишинга – выманивания персональных данных с помощью поддельных сайтов, иногда до мелочей копирующих внешний вид официальных ресурсов. Обойти стороной такие сайты поможет, в частности, плагин WOT (Web of Trust), доступный для всех основных современных браузеров: Internet Explorer, Firefox, Opera и Safari. Домашняя страничка программы – www.mywot.com. WOT располагает оперативно обновляемой базой адресов потенциально небезопасных сайтов. Его задача – предупредить вас о репутации того или иного веб-ресурса. Иконка WOT действует аналогично светофору: зеленый цвет – безопасный сайт, желтый – ресурс с удовлетворительной безопасностью, красный – вы рискуете найти на свою голову приключения. Заметим, что WOT работает в мягком, сугубо рекомендательном режиме и не блокирует какие-либо сайты автоматически – решения всегда принимает пользователь.

Списки WOT пополняются двумя путями. Во-первых, их поставляет известная своими антивирусными разработками компания Panda Security. Во-вторых, привлекаются социальные технологии: пользователи WOT имеют возможность выставлять собственные индексы безопасности для посещаемых ресурсов. Эти данные обобщаются, анализируются и используются для обновления списков.

Главная потенциальная опасность на веб-странице – это выполняемые на ней программы-скрипты. Вполне логично защититься от них каким-либо фильтром. Одно из лучших на сегодня решений этой задачи – дополнение NoScript (noscript.net). С его помощью можно серьезно повысить безопасность браузера Firefox. Назначение NoScript – блокировка самого разнообразного динамического контента. Данное дополнение умеет отключать JavaScript, Flash, обрабатывать объекты Microsoft Silverlight и элементы Iframe, блокирует загрузку исполняемых файлов, защищает от многих типов сетевых атак. NoScript отличается весьма гибкими возможностями настройки. По умолчанию он запрещает выполнение любых скриптов на открываемых страницах. С помощью значка NoScript в строке состояния браузера можно просмотреть список заблокированных на открытой веб-странице скриптов и разрешить выполнение только тех, которым вы доверяете. Списки доверенных ресурсов можно сохранять, причем как постоянно, так и только для текущей сессии работы с браузером, что весьма удобно. Кроме того, NoScript может автоматически добавить в «белый список» все сайты, которые сохранены в закладках вашего обозревателя. Поскольку настроек у дополнения действительно много, в нем предусмотрены инструменты их экспорта и импорта, а также создания их резервных копий.

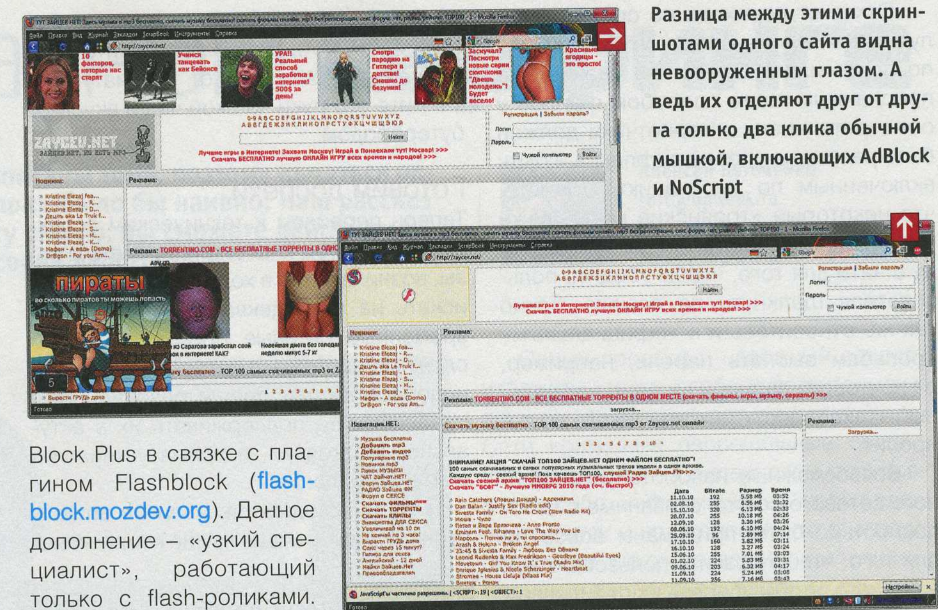
…Это достигается путем проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например от имени банков, служб или социальных сетей. В письме часто содержится прямая ссылка на сайт, неотличимый от настоящего. (Wiki)

Интернет-реклама также может стать угрозой безопасности. Даже если не вспоминать про ее навязчивость, она может использоваться для фишинга. Кроме того, многие ресурсы для демонстрации максимально эффективной рекламы стремятся собирать как можно более подробное досье о пользователях, включая сведения о просматриваемых веб-страницах, запросах интернет-поиска и других подобных вещах.

Пожалуй, наиболее мощное «лекарство» от интернет-рекламы – это дополнение AdBlock Plus (adblockplus.org). Кроме удаления собственно рекламы оно также обладает функциями контроля мультимедиаконтента на просматриваемых веб-страницах. AdBlock Plus способен справиться с рекламой, представленной в самых различных форматах, – от банальных баннеров до самых изощренных медиарешений.

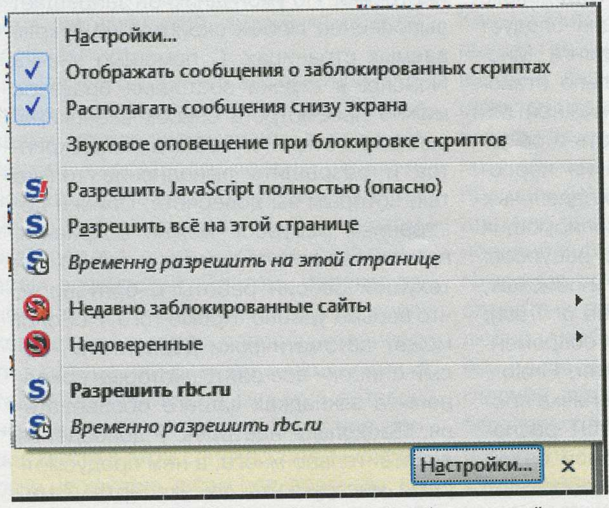
Работа с рекламой ведется в двух режимах. Основной – автоматический, на основе подписок – списков шаблонов рекламных источников и элементов. Предлагается порядка сорока подписок, оптимизированных для различных регионов, в том числе для России. Поскольку обновления подписок подгружаются при старте браузера, не стоит выбирать более двух-трех одновременно – это приведет к замедлению его работы. Второй режим работы – ручной. У нас есть возможность просто выделить на веб-странице ненужный фрагмент с рекламой и с помощью контекстного меню дать AdBlock команду создать на его основе новый фильтр.

Еще более заметных результатов можно добиться при использовании AdBlock Plus в связке с плагином Flashblock (flashblock.mozdev.org). Данное дополнение – «узкий специалист», работающий только с flash-роликами. При включенной защите на веб-странице вместо роликов демонстрируется пустой блок аналогичного размера, что сохраняет верстку просматриваемой страницы. Такой блок содержит кнопку, щелкнув по которой можно запустить заблокированный flash-ролик. Flashblock позволяет составлять «белые списки» сайтов, на которых вы хотите разрешить демонстрацию flash-элементов.



Разница между этими скриншотами одного сайта видна невооруженным глазом. А ведь их отделяют друг от друга только два клика обычной мышкой, включающих AdBlock и NoScript

Теперь займемся излишне любопытными веб-ресурсами, собирающими данные об активности юзера в Сети и вообще интересующимися личной жизнью пользователя. Обычно для этого применяются различные способы определения его IP-адреса, а также сохранение персональной информации с помощью cookie-файлов. Современные браузеры позволяют очищать списки таких файлов, однако это не обеспечивает полную защиту. Дело в том, что для сохранения персональной информации о пользователе все чаще применяются так называемые Local Shared Objects (LSO). Их иногда называют суперкуками, что вполне отражает их возможности. Дело в том, что они сохраняются не браузером, а flash-плагином. Поскольку «сберегаются» они в системных папках, такие файлы обычно защищены от удаления. Кроме того, это придает LSO кроссбраузерные возможности: они будут работать в любом используемом на компьютере браузере. Срок действия LSO может быть неограниченным, и такой объект способен хранить до 100 Кбайт данных, которые передаются по запросу внешнего сервера без какого-либо уведомления пользователя.



Плагин NoScript позволяет гибко управлять блокировкой динамического содержимого веб-страницы

Справиться с LSO способно дополнение BetterPrivacy (addons.mozilla.org/ru/firefox/addon/6623). Обычно после инсталляции и первоначального сканирования компьютера с интернет-подключением аддон находит до сотни таких объектов. При желании их можно сразу же удалить. После завершения каждого сеанса работы с Firefox дополнение BetterPrivacy демонстрирует отчет о количестве новых LSO-объектов, которые попытались сохранить посещенные сайты. У пользователя, соответственно, появляется возможность немедленно их удалить. При необходимости можно настроить BetterPrivacy на работу в автоматическом режиме, когда LSO-файлы будут удаляться без уведомления. Правда, если вы активно пользуетесь онлайновыми приложениями или играми, построенными на Flash, будьте осторожны с этой опцией, иначе вы рискуете потерять полезные сохраненные данные. Это дополнение поддерживает и более гибкие настройки. В диалоге LSO Manager можно просмотреть детальную информацию о найденных объектах: адрес сайта, сохранившего LSO, дату и время его сохранения. На основе этих и других сведений можно принимать обоснованные решения о блокировке или «сбереже-

RSS

Прокси-сервер (от англ. proxy – представитель, уполномоченный) – служба в компьютерных сетях, позволяющая клиентам выполнять косвенные запросы к другим сетевым сервисам. (Wiki)

нии» файла. При необходимости можно настроить удаление LSO по таймеру, что позволяет отделить LSO активно используемых вами веб-приложений от ненужных объектов.

Защищаем приватность

Современные технологии предлагают массу средств отслеживания поведения пользователя в интернете. Кроме того, они позволяют строить системы фильтрации контента, которые блокируют юзерам доступ к тем или иным ресурсам. Если вы не хотите становиться объектом такой слежки, не желаете, чтобы кто-либо узнал сайты, которые вы посещаете, или определял за вас, какие ресурсы вы можете просматривать, пора познакомиться с таким полезным объектом, как прокси-сервер. С его помощью можно повысить уровень анонимности при работе в Сети. Как ни странно, необходимость в таких решениях испытывают не только всевозможные киберзлодеи, но и вполне законопослушные пользователи.

Прокси-сервер, в самом общем случае, выступает в роли посредника между клиентом и удаленным ресурсом. Поскольку данные передаются через прокси, такой ресурс не может получить прямой доступ к адресу или персональным сведениям, которые можно извлечь из пересылаемых пользователем пакетов. Затрудняется и определение веб-сайтов, посещаемых юзером, поскольку пакеты идут на адрес прокси, который уже и перераспределяет их на нужные адреса. Таким образом, прокси-сервер помогает нам скрыть URL посещаемых сайтов и обойти многие системы блокировки трафика.

	Proxy	Port	Anonymity	Delay	Country	Https	Gateway	Danger	CoDeeN
✗	78.108.179.64	51177	---	---	~	~	~	~	~
✗	113.238.184.76	9415	---	---	~	~	~	~	~
✗	94.198.241.82	51490	---	---	~	~	~	~	~
✗	78.108.178.140	47736	---	---	~	~	~	~	~
✗	113.92.178.83	9415	---	---	~	~	~	~	~
✗	78.108.179.91	35217	---	---	~	~	~	~	~
✓	125.164.216.224	3128	Level 3	1530	~	~	~	~	~
✗	200.84.102.27	8000	---	---	~	~	~	~	~
✗	78.108.182.31	33100	---	---	~	~	~	~	~
✗	78.108.183.138	40895	---	---	~	~	~	~	~
✗	77.27.27.65	16589	---	---	~	~	~	~	~
✗	78.108.179.64	34080	---	---	~	~	~	~	~
✗	78.108.183.138	53752	---	---	~	~	~	~	~
✗	94.198.241.79	47647	---	---	~	~	~	~	~
✗	123.203.85.110	9415	---	---	~	~	~	~	~
✗	119.237.188.122	9415	---	---	~	~	~	~	~
✗	118.171.238.96	9415	---	---	~	~	~	~	~

Total	Level 1	Level 2	Level 3	Switch
300	1	0	1	0

Elite Proxy Switcher позволяет проверять списки прокси-серверов и быстро переключаться между ними в ходе серфинга

Прокси-серверы принято делить на несколько классов. «Прозрачные» прокси (transparent proxy) практически не влияют на приватность серфинга, реальный IP-адрес пользователя можно получить достаточно легко, поэтому их используют для вспомогательных целей. Анонимный прокси (anonymous proxy) уже способен скрыть реальный IP-адрес клиента, однако целевой веб-ресурс при некотором усилии его разработчика способен узнать об использовании клиентом прокси-сервера. В большинстве случаев это не мешает работе с ресурсами. Если же вы хотите скрыть не только свой адрес, но и сам факт использования прокси-сервера, вам нужен элитный прокси (elite proxy).

Указать адрес прокси-сервера можно в настройках любого современного браузера, однако здесь можно столкнуться с рядом проблем. Дело в том,

Заметим, что для надежной защиты одного прокси может оказаться недостаточно, поэтому те, кто действительно заинтересован в скрытности, строят цепочки из нескольких серверов.

что найти для себя бесплатный и рабочий прокси – не такая простая задача для обычного частного пользователя. Адреса доступных прокси-серверов могут достаточно часто меняться, поэтому и юзеру придется постоянно изменять настройки своего браузера. Гораздо удобнее воспользоваться одним из специализированных приложений для работы со списком прокси. В качестве примера мы рассмотрим программу Elite Proxy Switcher (www.eliteproxy-switcher.com).

Общаться с этой программой достаточно просто, не мешает даже отсутствие русского перевода интерфейса – все равно работать вы будете только мышкой. Сначала понадобится загрузить в софтину список адресов прокси, представленный в виде простого TXT-файла. После загрузки файла запускаем тестирование списка (кнопка Test the Selected Proxies). Будьте готовы к большому проценту отказов прокси из свободно распространяемых списков: десяток рабочих серверов на сотню-другую адресов – это нормальный результат. Для найденных рабочих прокси-серверов демонстрируются их адрес, а также скорость доступа. Колонка Anonymity показывает уровень защищенности прокси-сервера. «Level 1» обозначает элитный прокси, «Level 2» – анонимный, а «Level 3» – «прозрачный». Удобно, что список можно отсортировать по этому признаку. Остальные параметры в бесплатной версии скрыты.

Для начала работы с любым прокси достаточно просто выбрать сервер в списке и нажать кнопку Connect to This Proxy. В строке состояния браузера появляется строчка, в которой выводится адрес активного в данный момент сервера. Если в какой-то момент времени он становится недоступен, с помощью Elite Proxy Switcher можно быстро переключиться на следующий в списке. Есть в программе и режим автоматического переключения. В диалоге EPS Settings > Switch можно указать интервал времени, после которого софтина будет автоматически переходить на использование следующего в списке прокси.

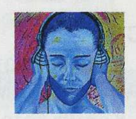
Как нетрудно заметить, основная проблема в использовании этой программы – это получение списка прокси для обработки. Elite Proxy Switcher предлагает возможность загрузки таких списков с сервера софтины одним кликом, вот только эта опция платная. Если вы не испытываете постоянной потребности в быстром обновлении, можно воспользоваться для получения первичных списков адресов такими открытыми сервисами, как proxy-list.org, freeproxylist.org, www.checker.freeproxy.ru и др. Подобных ресурсов довольно много, и они неплохо находятся интернет-поисковиками.

Заметим, что для надежной защиты одного прокси может оказаться недостаточно, поэтому те, кто действительно заинтересован в скрытности, строят цепочки из нескольких серверов. Однако это уже крайний случай, и для большинства нормальных задач такой уровень секретности не нужен. Существует также ряд других решений, связанных с использованием прокси. Например, на страницах UPgrade мы уже рассказывали о защищенном интернет-поиске с помощью системы Ixquick. Нельзя не вспомнить и о специализированной сети Tor или же веб-сервисах для анонимного серфинга. Однако эти решения вполне заслуживают отдельного рассказа. **UP**

…Сначала клиент подключается к прокси-серверу и запрашивает какой-либо ресурс, расположенный на другом сервере. Затем прокси-сервер либо подключается к указанному серверу и получает ресурс у него, либо возвращает ресурс из собственного кэша (в случаях, если прокси имеет свой кэш). (Wiki)

Сетка для пингвина

Реакция граждан, столкнувшихся с «мертвыми» сетевыми картами в среде Linux, нам известна: сами проходили через это. Есть еще девелоперы, выпускающие дистрибутивы, в которых для вызова к жизни работоспособных сетевушек нужна масса телодвижений.



Акустик
soft@upweek.ru
Mood: сломался бубен...
Music: no music

На наш взгляд, самым простым способом проверки жизнеспособности сетевых карт является запуск LiveCD / LiveDVD. Если система рапортует о доступных сетевых подключениях, то и славно. В противном случае советуем проверить, поддерживается ли вообще капризный сетевой адаптер, на ресурсах www.linux-drivers.org, www.linux-laptop.net и www.leenooks.com. Вполне возможно, что Linux-драйверы сетевой карты ждут не дождутся своего часа на сайте производителя. Не исключено, что проблема саботажа сетевушки давно решена (мы намекаем на Google, который знает почти всё).

Есть и более простые способы (хотя это кому как повезет). Так, например, в линейке Ubuntu может помочь «Менеджер проприетарных драйверов», предлагая автоматически установить компоненты для беспроводного модуля. Не забывайте о небольшом приложении ndiswrapper (sourceforge.net/projects/ndiswrapper, 200 Кбайт). Утилита призвана «оживлять» Wi-Fi-адаптеры, используя драйверы Windows. От вас нужно всего ничего: указать расположение INF-файла в папке с Windows-драйверами адаптера. Коль скоро и этот метод не привел к успеху, остается надеяться на обновленное ядро (www.kernel.org), в котором, не исключено, реализована поддержка вашей сетевой карты. Впрочем, современные дистрибутивы знакомы с огромным числом устройств, мы же будем считать, что проблемы с «дохлой» сетевушкой обошли вас стороной.

Сегодня мы постараемся убедить новичков в том, что подключение Linux-машины к интернету ничуть не сложнее аналогичного процесса в Windows. В нашем распоряжении кроме тестовых десктопа и ноутбука с установленной Ubuntu 10.04 беспроводной роутер ASUS WL-500W, коммуникатор HTC Touch 2 на базе Windows Mobile 6.5, смартфон HTC Desire под управлением Android 2.2 и мобильный модем Huawei E1552. Оставим в стороне специфические устройства (например, ADSL-модемы, подключенные к компьютеру посредством USB) и варианты подключений (например, VPN): маршрутизатор избавил нас (и наверняка избавит вас) от лишней работы.

По умолчанию подключенному компьютеру назначается динамический IP-адрес

Параметры широкополосного соединения нам автоматически установил мастер

На наш взгляд, самый простой способ – подключение компьютера к маршрутизатору Ethernet-кабелем: после загрузки операционной системы дополнительные манипуляции не требуются, поскольку машина уже в Сети. Хотя есть один нюанс: она использует динамический IP-адрес, полученный от щедрот DHCP-сервера роутера. Если требуется назначить компьютеру постоянный айпишник, к нашим услугам апплет Network Manager, значок которого расположен в трее.

Мы скомандовали «Изменить соединения» в контекстном меню этого значка, на вкладке «Проводные» выделили строчку нашего адаптера и нажали кнопку «Изменить». После этого на вкладке «Параметры IPv4» в списке «Метод» мы выбрали параметр «Вручную» и указали требуемые данные, включая адреса шлюза и DNS. Проверьте, активны ли чекбоксы «Подключать автоматически» и – при вашем на то благоволении – «Доступно всем пользователям». Если соединение пропало, перегрузите машину.

Как правило, для подключения к защищенной Wi-Fi-сети нужно всего ничего: щелкнуть левой кнопкой по значку Network Manager в трее и выбрать беспроводный ресурс. Для установления коннекта достаточно ввести ключ шифрования, поскольку современные дистрибутивы научились автоматически оп-

RSS: DNS (Domain Name System – Система доменных имен) – распределенная компьютерная система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста. (Wiki)

ределять протокол защиты. Более того, введенный пароль автоматически сохранится, и при последующих загрузках системы не будет нужды набирать его еще раз. Действия с назначением статического IP-адреса при беспроводном соединении не отличаются от рассмотренных выше (используйте вкладку «Беспроводная сеть» Network Manager).

Скучно, не правда ли? Как мы уже говорили, в большинстве случаев нет нужды в правке конфигурационных файлов. В некоторых дистрибутивах, например Pardus Linux (www.pardus.org.tr/eng) и PuppyRus (www.puppyrus.org), активацией сетевых подключений ведает специальный мастер, которому нужно дать ответы на пару-тройку вопросов – только и всего.

Пришла пора подключения Linux-машин к Сети при помощи мобильного модема. Мы поступили следующим образом: на вкладке «Мобильные широкополосные» менеджера сетевых подключений запустили «Мастер настройки» нажатием кнопки «Добавить». Нам потребовалось указать страну, мобильного оператора и тарифный план. Мастер автоматически заполнил необходимые поля (APN, имя пользователя и номер вызова) в параметрах соединения, за исключением поля для ввода пароля. При частом использовании мобильного коннекта советуем активировать чекбокс «Подключать автоматически».

После этого мы подключили мобильный модем к одному из USB-портов, и через несколько секунд система отрапортовала об установленном соединении. Обратите внимание на то, что, в отличие от компов с Windows, здесь мы не заморачивались установкой драйверов устройства. Практический совет: если система категорически не желает соединяться с Сетью, попробуйте подключить мобильный модем к другому USB-порту. Проверено – работает.

Смартфоны под управлением Android тоже могут принести пользу при подключении к интернету. Соединив телефон с «большим братом» USB-кабелем и выбрав в диалоге «Подключение к ПК» параметр «USB-модем», можно обойтись возможностями интернет-соединения, предоставленного сотовым оператором. Однако не следует забывать о врожденной «прожорливости» Android-устройств в отношении трафика и его негуманной стоимости.

Мы не беремся утверждать, что знаем все возможности всех Android-смартфонов, но тестовый HTC Desire с прошивкой 2.2 позволяет задействовать самое себя в качестве беспроводной точки доступа, к которой могут подключаться другие мобильные девайсы, например ноутбуки. На наш взгляд, данная функция пребывает в начальной стадии развития: невозможно изменить предлагаемые имя сети (HTC Network) и пароль (1234567890). Полагаем, нет смысла говорить о крайне низком уровне безопасности такого вида коннекта. Тем не менее после активации данной точки доступа подключение Linux-машин к беспроводной сети ничем не отличается от аналогичной процедуры с использованием Wi-Fi-маршрутизатора.

К сожалению, использование Android-смарфтона в качестве модема при подключении к тестовым машинам по протоколу Bluetooth оказалось невозможным. После установки пакета bluez-utils, расширяющего возможности системного инструмента, вы выяснили MAC-адрес смартфона командой `hcitool inq` (пусть это будет 00:00:00:00:00:00), после чего затребовали список «голубозубых» служб, поддерживаемых Android-устройством (команда `sdptool browse 00:00:00:00:00:00`). Увы, Dial-up Networking Gateway в полученном списке не оказалось.

Зато коммуникатор на базе Windows Mobile справился с должностью bluetooth-модема. В некоторых сетевых источниках рекомендуется пакет gnome-ppp, мы же предпочли установить альтернативный bluetooth-менеджер Blueman (blueman-project.org). Сначала мы отредактировали содержимое файла rfcomm.conf так, как это советуют на forum.ubuntu.ru/index.php?topic=11109.0, после чего «познакомили» bluetooth-модули компьютера и коммуникатора. Затем мы вызвали настройки сети в окне локальных служб Blueman, где отключили чекбокс «Групповая сеть» и активировали чекбокс «Точка доступа к сети (NAP)».

Для подключения компьютера к интернету мы использовали команду «Настройка» контекстного меню коммуникатора, выбирая параметр «Передача данных через модем (DUN)» (после подключения ПК к Сети на экране аппарата появлялся индикатор Dial-up Networking). Что и говорить, манипуляции с Bluetooth не очень-то просты. Впрочем, никто не запрещает подключить коммуникатор на базе Windows Mobile к USB-порту компьютера: и проще, и быстрее.

Теперь расскажем о создании общего доступа к файлам и папкам в среде GNU / Linux. Для этой задачи нам понадобится компонент по имени Samba, который давно поселился в репозиториях большинства дистрибутивов. Несмотря на обилие различных графических оболочек, позволяющих без особых проблем настроить общий доступ, результатом их работы является внесение изменений в конфигурационный файл /etc/samba/smb.conf? (для развития кругозора советуем ознакомиться с материалом на unixforum.org/index.php?showtopic=24962).

Инструменты оконной среды GNOME современных дистрибутивов позволяют настроить общий доступ за считанные секунды. В контекстном меню папки мы воспользовались командой «Общий доступ», после чего Ubuntu предложила нам установить нужную службу (необходимые компоненты были загружены автоматически из репозитория). После этого мы согласились с автоматическим назначением прав, дали имя ресурсу и включили гостевой доступ (последнее действие не является обязательным условием, но для домашней сети окажется актуальным). После нажатия кнопки «Создать ресурс» общая папка появилась в «Сетевом окружении» компьютера под управлением Windows XP, подключенного к тестовому маршрутизатору.

И напоследок: для доступа к «расшаренным» папкам на Windows-машинах от вас не потребуется дополнительных манипуляций. Отправляйтесь в каталог «Сеть» файлового менеджера Linux-компьютера, где вас уже ждут Windows-ресурсы общего доступа.

Итак, мы убедились, что процедура проводного подключения Linux-машин ничуть не сложнее аналогичных действий в Windows: как правило, сразу после загрузки системы компьютер оказывается соединен с Сетью. Для подключения к защищенной беспроводной сети достаточно ввести ключ шифрования. Нужные параметры соединения в случае с мобильным модемом за вас укажет мастер. Для использования в качестве модема Android-смартфона, подключенного к USB-порту, нужен один клик. Разумеется, наше оборудование пришлось по душе «пингвину», да и ядро используемой системы у нас вполне свежее.

В общем-то, мы не собираемся призывать вас к немедленной миграции на Linux. Просто в ряде случаев засада подстерегает нас вовсе не там, где она ожидалась. **UP**

DHCP (Dynamic Host Configuration Protocol – протокол динамической конфигурации узла) – это сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Данный протокол работает по модели «клиент-сервер». (Wiki)

Инетомобиль

Наш журнал никогда не спровоцирует международный скандал. Однако мы не в силах удержаться от новости из одной сопредельной страны. Только не смейтесь. Наш эстонский коллега Свен Вахар, тестируя смартфон, умудрился «попасть» почти на 1100 евро.



Акустик
soft@upweek.ru
Mood: смех сквозь слезы
Music: no music

Нет, происхождение телефона вполне себе легитимно, да и тестер не баловался звонками в различные сервисы для услады души и тела. Все намного прозаичнее: в эту дикую сумму нашему, с позволения сказать, коллеге обошелся мобильный трафик, расходуемый как системными, так и сторонними приложениями (rus.delfi.ee/daily/business/article.php?id=33427533). И это при том, что в маленькой, но отчаянно гордой стране три оператора мобильной связи предлагают безлимитные пакеты для подключения к интернету всего за 6 евро в месяц. Один из таких пакетов (настоящий анлим, без оговорок) юзает и автор этих строк на той же модели смартфона.

Россиянам, большая часть которых использует предоплаченные разговорное время и мобильный трафик, проще: исчезли со счета несколько сотен рублей – так невелика потеря. Хотя, мы согласны с вами, обидно. Владельцы устройств на базе Symbian и Windows Mobile находятся в более выигрышном положении: программы для этих систем, будучи выгруженными из памяти, не склонны к самостоятельному выходу в Сеть и, как следствие, не транжирят драгоценный трафик.

Увы, специфика смартфонов под управлением Android изначально подразумевает постоянное соединение с интернетом. Сказывается тесная интеграция с учетной записью Google и мерзкой особенностью приложений «возрождаться» после выгрузки. Казалось бы, что может быть проще полного запрета подключения? В настройках Android-устройств достаточно выключить чекбокс «Мобильный интернет» – и можно забыть об алчности повелителей мобильного трафика. Но в этом случае проще пользоваться обычным мобильным телефоном без функции подключения к Сети.

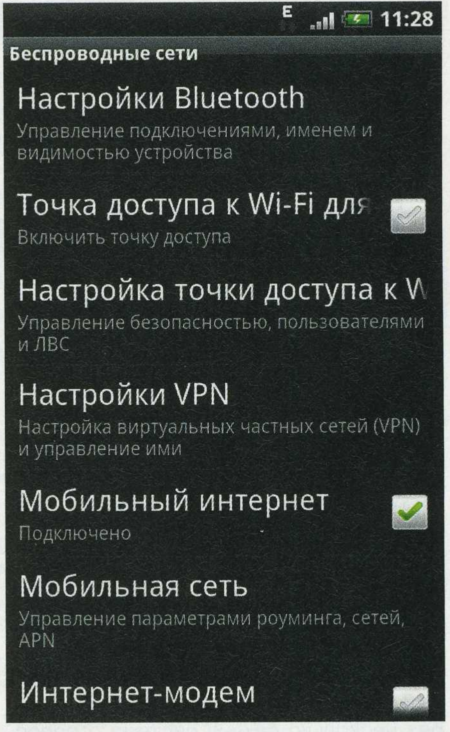
Вы спросите: а кто запрещает работать с Wi-Fi-соединением, тем более что все современные девайсы поддерживают эту технологию? Отвечаем: вы правы, Wi-Fi никто не отменял, но попробуйте найти бесплатную точку доступа, например, в Германии – тот еще квест. А что говорить про российскую глубинку… Понятно, что лучшим решением станет домашний беспроводный роутер, однако в других условиях халявное Wi-Fi-соединение не гарантировано. В конечном итоге, на наш взгляд, главным видом соединения для смартфонов и коммуникаторов все равно остается т. н. мобильный интернет, или услуга подключения к Сети, предоставляемая оператором сотовой связи.

Как правило, все параметры мобильного коннекта настраиваются автоматически. Если не получилось – требуйте необходимые данные от поставщика связи. Настройка Wi-Fi-коннекта для Android-устройств сводится к вводу ключа шифрования для защищенных сетей, аналогичная процедура для Symbian-девайсов ничуть не сложнее. К слову, в свое время автору этих строк потребовалось установить альтернативную прошивку для маршрутизатора ASUS WL-500W, поскольку с заводской микропрограммой роутер отказывался «дружить» с Nokia N82.

Наиболее занудливой процедурой соединения с точкой доступа Wi-Fi нам показались действия при настройке подключения на коммуникаторах под управлением Windows Mobile: все-таки несколько операций и ввод длинного ключа шифрования при помощи стилуса не очень способствуют хорошему настроению. Нам пока неизвестно, как выглядит настройка Wi-Fi-соединения в Windows Phone, – надеемся, что упомянутая архаика в новой мобильной системе канет в Лету.

«Черные дыры» для мобильного трафика

Вряд ли у вас возникнут трудности при ручном вводе параметров мобильного или Wi-Fi-соединения. Точно так же мы не думаем, что все наши читатели используют на своих телефонах безлимитное интернет-соединение (тем не менее настоятельно советуем присмотреться к действующим тарифам). Если же анлим уже поселился на вашем устройстве (как, впрочем, и на нашем тестовом смартфоне), львиная доля этого текста не для вас. Кстати, стоит помнить о том, что в некоторых странах цена мобильного трафика зашкаливает за 4 евро за 1 Мбайт (мы не оговорились).



Лекарство от затрат – отключение мобильного интернета

Выше мы упоминали о том, что устройства на базе Windows Mobile и Symbian не грешат самовольным подключением к интернету, но это в общем случае. Так, например, наш второй тестовый коммуникатор HTC Touch 2 с оболочкой TouchFLO 2D содержит погодный информер, в настройках которого изначально активировано автоматическое обновление прогноза. По заверениям разработчиков, расход трафика смехотворен – всего-то несколько килобайт для одного апдейта, но интервал между ними не ука-

RSS

Windows Phone 7 (кодовое название – Photon) – операционная система Windows Mobile, разработанная Microsoft и основанная на Windows Embedded CE 6.0, выход которой состоялся в октябре 2010 года. (Wiki)

зан: сколько трафика и денег «утечет» за месяц, можно только гадать.

То же относится и к другим погодным приложениям как для Windows Mobile, так и для Symbian. Понятно, что загрузка метеорологического прогноза в роуминге еще больше опустошит ваш счет. Рецепт очевиден: отключение автоматического обновления данных. В конце концов, если вы не профессиональный синоптик (к слову, маркетологи произошли именно от синоптиков, мы в этом уверены), то не грех загрузить погодные апдейты вручную или при подключении посредством Wi-Fi.

По нашему мнению, главными потребителями трафика являются программы, установленные в телефоне. Вот только не нужно гнобить проприетарный софт: если уж более чем свободный десктопный веб-браузер Chromium не гнушается сбором данных о пользователях (а это, как вы понимаете, все тот же трафик), то что говорить о великом множестве мобильных приложений.

Если программа, нуждающаяся в соединении с интернетом, по завершении работы корректно выгружается из памяти (особенно это касается Windows Mobile), то и замечательно: за несколько лет создания обзоров мобильных приложений для WM и Symbian нам не встречались продукты, тихой сапой выходившие в Сеть. Другое дело – встроенные рекламные модули, расходующие трафик. Однако мы не припоминаем сколь-нибудь значимого числа программ для Windows Mobile и Symbian, грешащих тягой к рекламе. А вот софт для Android…

Даже «голый» Android, без стороннего софта, является «черной дырой» для мобильного трафика. Хотите получить доступ к Android Market? – извольте указать параметры своей учетной записи Google. Указали? Получите автоматическую синхронизацию нужных и ненужных сервисов с телефоном. Ко всему прочему смартфоны от HTC с фирменной оболочкой Sense немедленно потребуют свой кусок трафика для обновления – вы угадали – прогноза погоды.

По наблюдению автора этого текста, тестовый HTC Desire без сторонних программ и веб-серфинга расходовал около 6 Мбайт трафика в сутки. Если же включить клиентские приложения для социальных сетей (Twitter и Facebook), то дополнительные расходы нетрудно предугадать. Количество сторонних Android-программ, бесплатные версии которых несут на борту рекламные модули, превысило все разумные пределы. Остается либо мириться с ситуацией, либо использовать т. н. профессиональные модификации тех же приложений, но за дополнительные деньги.

Другая особенность приложений для Android – их способность жить своей неприметной жизнью в фоновом режиме со всеми последствиями. Одна часть продуктов успешно «прибивается» либо системным инструментом, либо сторонним менеджером задач, например Advanced Task Killer (sites.google.com/site/rechildmobi), но другая часть, подобно птице феникс, через какое-то время возрождается вновь. Особым цинизмом отличалась Android-версия Skype, о которой мы недавно рассказывали.

Мало того что после использования программной кнопки «Выход» софтина и не думает убираться с глаз долой, так еще различные Task Killer оказываются бессильными перед энтузиазмом Skype, который немедленно загружается в фоновом режиме. Казалось бы, зачем нужно подобное рвение? На наш взгляд, все объясняется применением пиринговых технологий разработчиками Skype. Другими словами, наши компьютеры и смартфоны задействуются в качестве шлюзов для обмена данными (разумеется, с расходом трафика). Кстати, в Skype и не думали скрывать эту особенность (www.skype.com/intl/ru/support/user-guides/p2pexplained).

http://m.odnoklassniki.ru/dk;jsessi...
одноклассники.ru
[redacted]
17:50
История статусов (0)
Друзья на сайте (0)
Сообщения
Обсуждения
Гости
Оценки фотографий
Мои друзья (45)
Дни рождения друзей (1)

Используйте веб-страницы, адаптированные для мобильных устройств

Экономная экономика

Наилучший способ экономии затрат мобильного трафика – безлимитный пакет (уж простите за назойливость). Если такового не предвидится, рекомендуем установить веб-браузер Opera Mobile (www.opera.com) с технологией Opera Turbo, позволяющей сжимать данные до 80% при помощи серверов компании Opera Software (не забудьте проверить в настройках, включена ли эта функция). Второй способ снижения затрат – использование веб-страниц, адаптированных для мобильных устройств. Например, практически все популярные веб-сервисы предлагают такую возможность.

Типичный пример – «Одноклассники», для которого, кстати, пока еще не выпущен Android-клиент. Мобильная версия данного ресурса вполне себе функциональна, особенно на экранах с большим разрешением. Как правило, URL мобильных сайтов выглядят как pda.site.ru, m.site.ru или wap.site.ru. Посмотрите внимательно на титульные страницы любимых ресурсов – наверняка вы найдете ссылку вида «Мобильная версия».

Не исключено, что штатный веб-браузер по умолчанию загружает изображения, пусть и небольшие. Десяток-другой таких картинок израсходуют ощутимую долю мобильного трафика. Не оставляйте «без присмотра» выгруженные программы на Android-устройствах: возможно, эти приложения притаились в фоновом режиме и бесцельно расходуют мегабайты. Особого внимания заслуживают софтины с рекламными модулями.

Аппетиты каждой программы нетрудно выяснить при помощи специальных утилит, например TrafficStats (www.cyrket.com/p/android/com.trafficstats). Статистику расхода трафика по заданным промежуткам времени предоставит софтина NetCounter (www.jaqpot.net/netcounter). Существует и более радикальный метод борьбы с утечкой трафика на Android-смартфонах – запрет сетевой активности для определенных программ. Таким искусством владеет, например, DroidWall (code.google.com/p/droidwall), но для работы этого приложения требуются права суперпользователя.

Однако главным инструментом при экономном расходовании мобильного трафика является – не поверите – сам пользователь, поскольку конструктивную работу мысли пока никто не отменял. **UP**

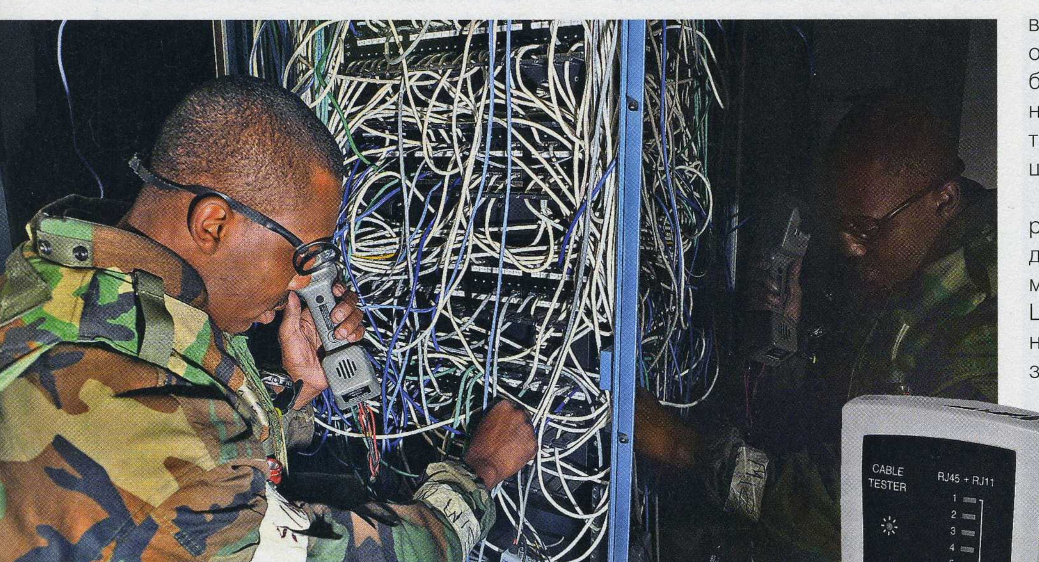
HTC Sense – пользовательский интерфейс, разработанный компанией HTC для мобильных устройств с операционными системами Android и Windows Mobile. Основан на предыдущей оболочке от HTC под названием TouchFLO 3D, которая применялась в телефонах на Windows Mobile. (Wiki)

Не **работает** сеть?

Причин неработоспособности проводной локальной сети в среде Windows может быть множество. Поэтому в данном случае я попытаюсь предложить не какое-то уже готовое универсальное решение, а пошаговую технологию самостоятельного поиска виновника сбоя.



Сергей Трошин
problem@upweek.ru
Mood: устал
Music: тишина



Причем технология эта по большей части будет работать как при диагностике самой последней версии Windows, так и в более старых ее вариациях.

«Медные» проблемы

Если ни «Восстановление системы», ни беглый осмотр настроек сети не принесли никаких результатов, то начинать диагностику следует все-таки с проверки оборудования и наличия физического соединения. Это легче и гораздо быстрее, нежели ковыряться в потрохах Windows. Самое простое – взгляните на светодиодные индикаторы сетевых карт и маршрутизаторов: есть ли сигнализация о подключении устройств и передаче данных? Если где-то не горит соответствующий светодиод, то, скорее всего, система ни при чем, а, например, неисправен (или выскочил из гнезда) сетевой провод. Может даже потребоваться более качественный кабель, или, возможно, надо будет заново обжать на уже имеющемся другие сетевые разъемы (если позволяет длина), после чего прозвонить кабель специальным тестером.

Проверьте правильность распайки кабеля (смотрите схемы на ru.wikipedia.org/wiki/Витая_пара). Не забудьте, что при соединении компьютеров напрямую, без коммутатора, может потребоваться другая схема разводки – перекрестная (Crossover). Также может «выгореть» порт на коммутаторе (из-за грозы, например, или обрыва питания) – в этом случае поможет переключение кабеля в свободное гнездо. Иногда помогает вернуть к жизни коммутатор или сетевую карту полное их обесточивание на несколько минут – с выдергиванием компьютера из розетки. Можно даже попробовать переставить сетевую карту в другой слот или просто «передернуть» – возможно, причина сбоя в плохом контакте. Кроме того, нелишним будет сбросить настройки маршрутизатора (особенно если сеть беспроводная) в «заводское» состояние, а также обновить его прошивку. Кстати, в случае беспроводной сети пытайтесь для начала наладить соединение сразу после ресета точки доступа, не используя никакого шифрования.

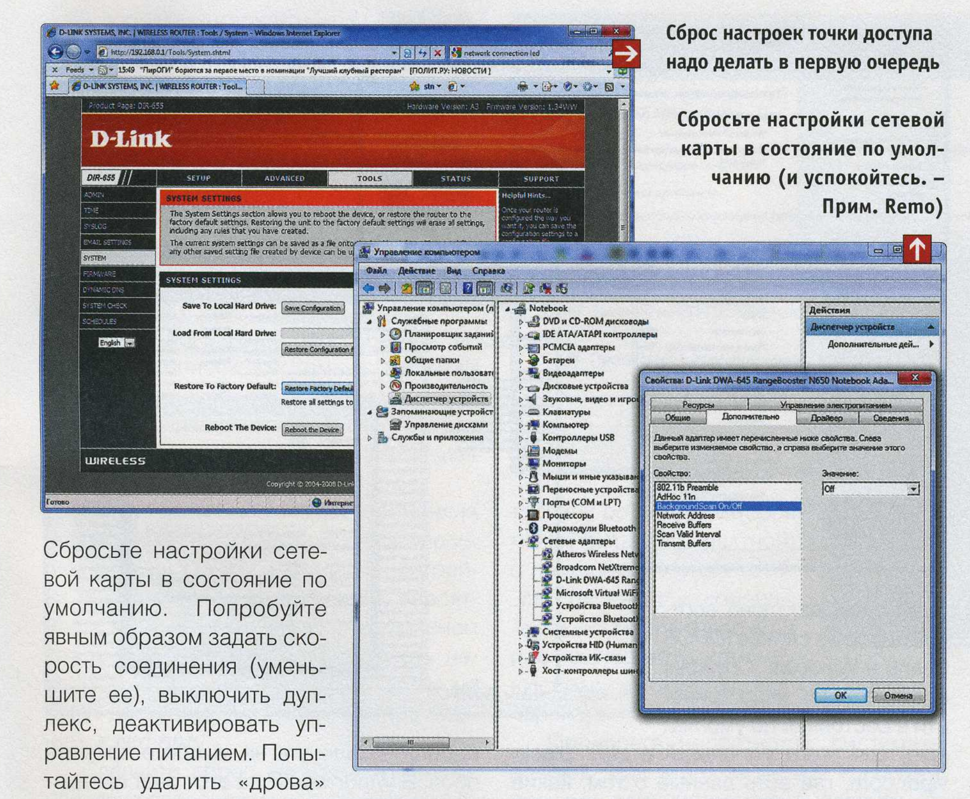
Наконец, проверить исправность оборудования можно, протестировав его в другой сети, например у приятеля. Либо можно взять какой-нибудь «линуксовый» LiveCD и посмотреть, будет ли функционировать сеть под другой ОС. Если все заработает, значит, оборудование уж точно ни при чем. Кстати, не стоит забывать, что причиной сбоев и нестабильной работы сети могут быть внешние электромагнитные помехи – идущий рядом с сетевым кабелем электропровод или некачественная микроволновка рядом с точкой доступа (а также многочисленные точки доступа соседей – выбирать лучше наиболее свободный канал, в этом поможет программа inSSIDer (metageek.net/products/inssider). Наконец, попробуйте временно отказаться от роутера и соединить два ПК напрямую коротким патчем или подключиться к интернету без маршрутизатора.

Дела программные

Таким образом, мы исключили из возможных причин сбоя неисправность оборудования, а также убедились, что кабель качественный и идеально обжат. Можно переходить к диагностике программной части. Например, проверить правильность установки «дров» для сетевой карты. Откройте «Диспетчер устройств» и убедитесь, что там ничто не сигнализирует о проблемах с драйверами, конфликте прерываний (некоторым сетевушкам не нравится IRQ15) или адресов ввода-вывода.

RSS

ping – утилита для проверки соединений в сетях на основе TCP/IP. Она отправляет запросы (ICMP Echo-Request) протокола ICMP указанному узлу сети и фиксирует поступающие ответы (ICMP Echo-Reply). (Wiki)



Сброс настроек точки доступа надо делать в первую очередь

Сбросьте настройки сетевой карты в состояние по умолчанию (и успокойтесь. – Прим. Remo)

Сбросьте настройки сетевой карты в состояние по умолчанию. Попробуйте явным образом задать скорость соединения (уменьшите ее), выключить дуплекс, деактивировать управление питанием. Попытайтесь удалить «дрова» сетевой карты и поставить их заново (желательно предварительно вычистив из реестра следы его предыдущей установки). Причем тут лучше протестировать два разных драйвера – самый последний от производителя компьютера или ноутбука и самый последний от производителя сетевой карты или ее чипсета (например, от Atheros для Wi-Fi-карт на данном чипсете). Самые свежие «дрова» последнего типа можно найти на сайтах forums.laptopvideo2go.com и station-drivers.com. Если же в вашем ПК несколько сетевых адаптеров, то убедитесь, что вы их не перепутали. Попробуйте отключить адаптер, который вы не используете. Разумеется, есть смысл наведаться и на Windows Update – возможно, там обнаружился какой-то патч или обновленный драйвер, который избавит вас от сбоя. Так, поддержка WPA2 в Windows XP появится только после обновления системы и «дров» адаптера.

И все-таки это Windows

Итак, вы убедились, что оборудование и кабели в норме, а драйверы сетевой карты установлены и функционируют корректно. То есть сам коннект есть, а сеть не работает. Приступаем к самой сложной части процесса – проверке настроек сети в Windows. Это следует сделать, даже если вы их уже неоднократно проверили до этого. Но для начала обязательно отключите все файрволлы (в том числе штатный брандмауэр Windows) и антивирусы, а лучше вообще временно удалите их. Некоторые «огненные стены» при сбоях блокируют работу сети даже в отключенном состоянии. И учтите, что функционирование локалки (и тем более интернета) могут нарушать и вирусы, так что непременно просканируйте систему, перед тем как приступить к диагностике. Лучше всего – парой разных антивирусов. Далее в диалоге «Свойства системы» > «Имя компьютера» обратите внимание на имя компа и рабочую группу – у каждого ПК домашней сети должно быть уникальное имя, а название рабочей группы у них должно совпадать, причем желательно все это записывать заглавными буквами латинского алфавита, без пробелов и спецсимволов, длина должна составлять не более 15 букв.

Затем перейдите в «Центр управления сетями и общим доступом» в «Панели управления» и выберите раздел «Изменение параметров адаптера», после чего откройте диалог свойств вашего сетевого соединения. Удостоверьтесь, что для него установлены следующие сетевые компоненты (на примере Windows 7).

1. «Клиент для сетей Microsoft». Если его нет, то нажмите кнопку «Установить» и установите его.

2. «Планировщик пакетов QoS» – этот компонент помогает при использовании голосовых и видеоконференций, а также при работе с мультимедиапотоками, хотя на время диагностики сети его можно и отключить.

3. «Служба доступа к файлам и принтерам сетей Microsoft» – устанавливайте ее, только если необходимо предоставить в общий доступ файлы и принтеры данного ПК.

4. «Протокол интернета версии 6 (TCP/IPv6)» – этот протокол пока мало используется (в Windows XP он по умолча-

Также пингом иногда ошибочно называют время, затраченное на передачу пакета информации в компьютерных сетях от клиента к серверу и обратно от сервера к клиенту. Это время называется лагом (англ. отставание; запаздывание), или собственно задержкой, и измеряется в миллисекундах. (Wiki)

нию не установлен), на этапе диагностики его можно отключить.

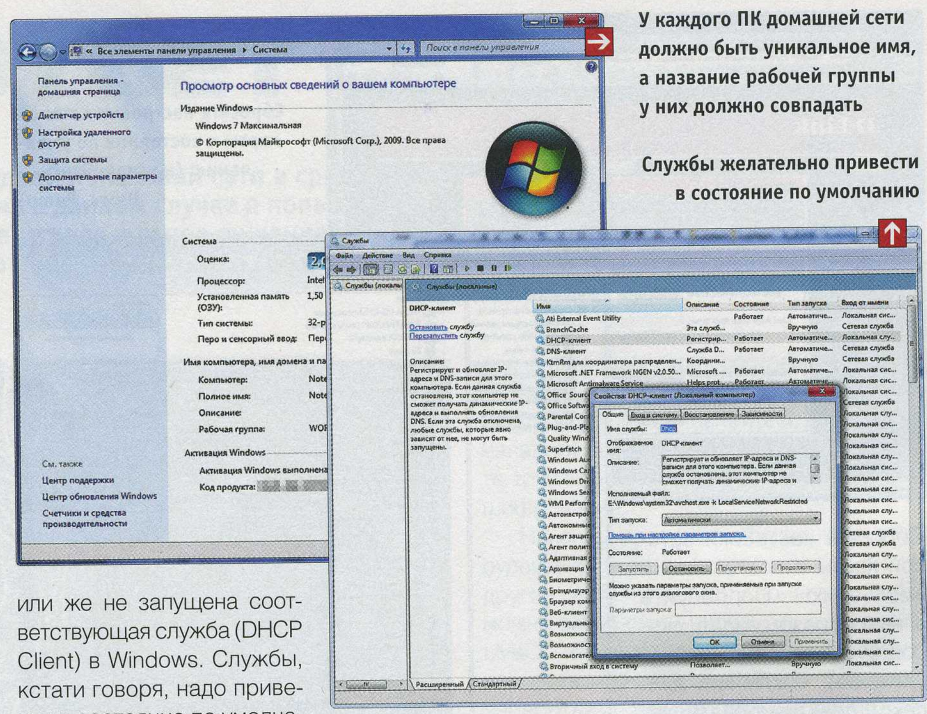
5. «Протокол интернета версии 4 (TCP/IPv4)». В соответствии с конфигурацией вашей сети либо задайте в его настройках явным образом IP-адрес и маску подсети (например, 192.168.0.10 и 255.255.255.0), либо используйте автоматическое присвоение IP, которое осуществляет сервер DHCP, работающий в вашем маршрутизаторе. Проверьте, чтобы маски на всех ПК сети совпадали, а айпишник у каждого компа был собственный (то есть у первого ПК – 192.168.0.10, у второго – 192.168.0.11 и так далее, а у маршрутизатора – обычно 192.168.0.1). Проверьте правильность установленных IP шлюза и DNS-серверов (если дома есть маршрутизатор, то обычно это его айпишник). Нажмите кнопку «Дополнительно» и попробуйте на странице WINS снять флажок «Включить просмотр LMHOSTS» (если в настройках вашей сети этот файл не используется). Попробуйте установить параметр «Включить NetBIOS через TCP/IP».

6. «Драйвер в/в тополога канального уровня» и «Ответчик обнаружения топологии канального уровня» можно пока отключить (в Windows XP их и нет), они используются для отображения схемы сети. Впрочем, если сеть частично все-таки работает, то систему можно попросить построить такую схему – возможно, она подскажет, на каком участке затык.

Учтите, что, например, в Windows XP драйвер сетевой карты может устанавливать и другие компоненты (например, Jumpstart Wireless Intermediate Driver, Wireless Intermediate Driver). Если вы найдете в этом списке что-то, кроме вышеперечисленного, то с помощью Google постарайтесь разобраться, что это такое и для чего это нужно. Попробуйте деактивировать все лишнее. На вкладке «Доступ» свойств соединения временно отключите общий доступ к интернету, если вы его используете.

Вернитесь к списку сетевых соединений и, выбрав свое, вызовите в его контекстном меню диалог «Состояние». Еще раз проверьте все параметры, которые увидите в этом окне, а также на странице «Сведения о сетевом подключении». Здесь все должно быть так, как задумано вами при настройке сети. То есть правильные IP, маска, шлюз, DNS и так далее.

Так, если вы видите, что IP-адрес не назначается автоматически, значит, проблема может быть в DHCP-сервере роутера,

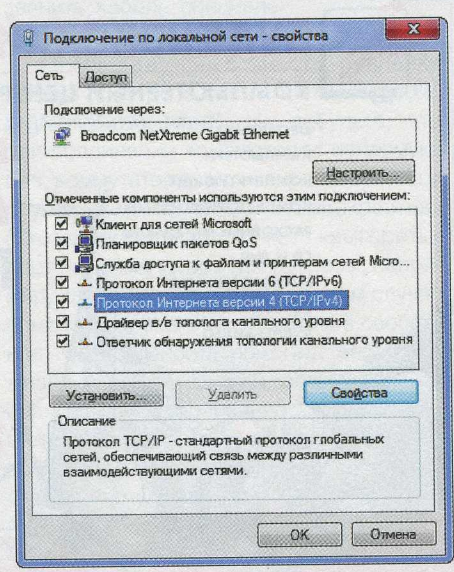


У каждого ПК домашней сети должно быть уникальное имя, а название рабочей группы у них должно совпадать

Службы желательно привести в состояние по умолчанию

или же не запущена соответствующая служба (DHCP Client) в Windows. Службы, кстати говоря, надо привести в состояние по умолчанию, для этого используйте сайт blackviper.com, где есть данные о том, какие из них должны быть изначально включены, а какие выключены.

В Windows 7 предусмотрено средство автоматической диагностики сети – его можно вызвать через диалог «Состояние», оно же «добывается» через контекстное меню индикатора сети в системном трее. Попробуйте им воспользоваться. По окончании тестирования непременно загляните в отчет «Просмотреть дополнительные сведения» – там может содержаться информация, способная натолкнуть на мысли о причине сбоя. В Windows XP на этот счет предусмотрена только команда «Исправить», с ней попытать счастья также стоит, как и с командой `netsh diag gui`. И скачайте простую диагностическую утилиту на support.microsoft.com/kb/914440/en-us. Кроме того, в Windows, в «Центре управления сетями и общим доступом» имеется команда «Устранение неполадок» – в борьбе со сбоем все средства хороши, даже самые примитивные.



Настройки протоколов TCP/IP придется перепроверить

К последнему этапу можно приступать после того, как вы убедились, что и оборудование в порядке, и драйверы в норме, и файрволлы не мешают, и в автозагрузке с помощью `msconfig` все отключено, и вирусов нет, и даже настройки роутера и самой сети на локальных клиентах абсолютно верные. В этом случае причина сбоя может крыться в повреждении самой операционной системы или ее конфигурации. Для начала попробуйте классический `ping` (по большому счету, его надо было пробовать еще до начала всей диагностики, чтобы понять, что же конкретно не работает). Сначала проверьте, функционирует ли сеть в пределах одного вашего ПК: `ping 127.0.0.1` и `ping 192.168.0.10` (считаем, что адрес проблемного компа – 192.168.0.10). Если это работает и вы получаете ответ, то снова проверяйте соединение с роутером, другими компьютерами сети и смотрите, на каком этапе `ping` проходить перестанет. Точно так же следует прове-

RSS

IPv6 (англ. Internet Protocol version 6) – новая версия протокола IP, призванная решить проблемы, с которыми столкнулась предыдущая версия (IPv4), за счет использования длины адреса 128 бит вместо 32. (Wiki)

рить доступ к интернет-шлюзу, DNS-серверам роутера и провайдера. Не исключено, что вы все-таки не там ищете и виновато другое устройство или кабель. Разумеется, если пинги между всеми ПК сети проходят, то, скорее всего, от проблемы вы уже избавились и сеть функционирует! В этом случае думайте о том, работа какого конкретно компонента (протокола) сети вас не устраивает, и разбирайтесь уже с ним.

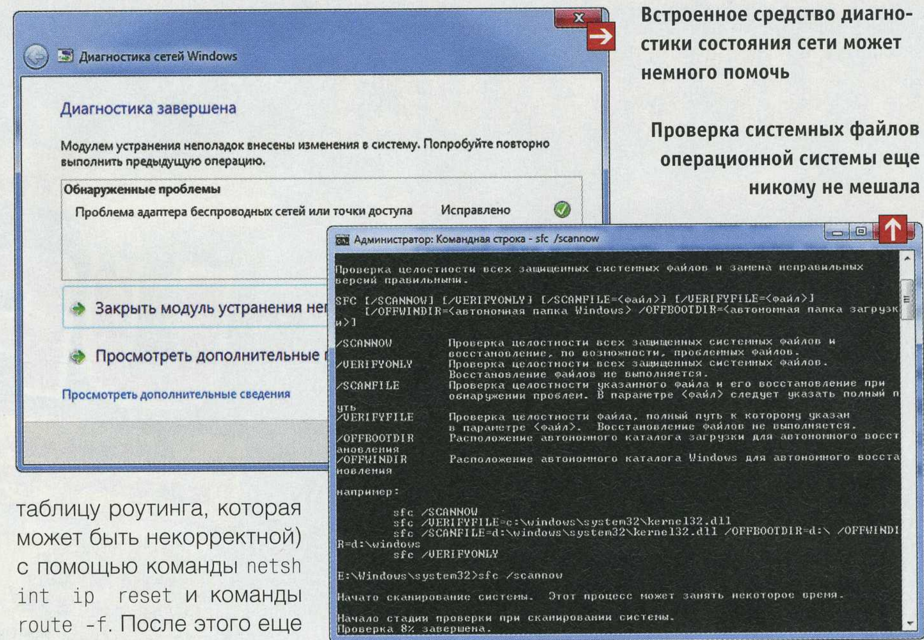
Крайне полезно на данном этапе заглянуть в список системных событий («Панель управления» > «Администрирование» > «Просмотр событий») – вполне возможно, именно там вы получите данные о причине сбоя.

Попробуйте вспомнить, применяли ли вы какие-либо твики системы (и особенно твики TCP/IP), меняли ли настройки роутера. Высока, например, вероятность того, что при неверно выбранном параметре `MTU` сеть будет работать некорректно или же некоторые сайты не будут доступны. Так что лучше все вернуть к дефолту.

Сделайте сброс настроек и восстановление первоначальной конфигурации LSP Winsock с помощью команды `netsh winsock reset catalog`. В некоторых случаях она оказывается самым простым и быстрым спасением. Также есть смысл сбросить настройки TCP/IP (в частности, таблицу роутинга, которая может быть некорректной) с помощью команды `netsh int ip reset` и команды `route -f`. После этого еще раз выполните команду «Исправить» в свойствах соединения и перегрузите ПК.

Проверьте целостность системных файлов. Для этого запустите консоль с правами администратора и введите команду `sfc /scannow`. Ну, и последний шанс установить источник проблем – попробовать переустановить Windows.

Вот, собственно, и все основные шаги по поиску причины сбоя. Самое главное же – понять, где и что надо искать. Сама фраза «не работает сеть» может толковаться по-разному. От «не видны «расшаренные» папки» до «не работает DNS» и «недоступен прокси». А это отнюдь не то же, что и «нет физического соединения». Так что, перед тем как все это проделывать, присядьте и еще раз спокойно подумайте: что же все-таки (и где) на самом деле не работает? UP



Встроенное средство диагностики состояния сети может немного помочь

Проверка системных файлов операционной системы еще никому не мешала

CLASSIFIEDS

В журнале UPgrade появилась новая рекламная рубрика Classifieds. Мы придумали ее специально для того, чтобы расширить возможности наших партнеров. Главное преимущество данной рубрики – низкая стоимость размещения информации о ваших продуктах в нашем журнале.
За дополнительной информацией следует обращаться к Татьяне Бичуговой по телефону (495) 681-7445, e-mail: bichugova@veneto.ru.

Журнал UPgrade всегда рад людям, готовым влиться в ряды наших авторов. Если вы считаете, что можете писать интересные тексты, то, возможно, вы правы! Людям «железных» интересов надо писать на адрес platon@upweek.ru непосредственно Платону Жигарновскому.
Тем, кто стремится описывать телекоммуникации, смартфоны и прочие мобильные штуки, а также обычный софт, обращаться следует по другому почтовому адресу – b@upweek.ru (к Николаю Барсукову). Тема письма «Новый автор» существенно все облегчит, поскольку нам приходит просто неприличное количество спама.
Письма на ящике upgrade@upweek.ru также внимательно и с интересом нами прочитываются.

Расценки на размещение рекламы в рубрике Classifieds (НДС включен)

Формат	Размер, мм	Стоимость, у. е.
1/4	184 x 56	500
1/4	90 x 117	500
1/8	90 x 56	350
1/16	43 x 56	190
1/16	90 x 26	190
1/32	43 x 26	130

В настоящее время протокол IPv6 уже используется в нескольких сотнях сетей по всему миру (более 3000 сетей на июль 2010 года), но пока еще не получил столь широкого распространения в интернете, как IPv4. (Wiki)